100 Q&As

ON CYBER SECURITY LAW OF
THE PEOPLE'S REPUBLIC OF CHINA

中华人民共和国
网络安全法
百问百答

左晓栋◎主编

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内容简介

本书针对社会各方面对《中华人民共和国网络安全法》（本书简称《网络安全法》）的关切，整理了100个问题，并给出了回答。按照各项问答对应的《网络安全法》条款的顺序，将这些问答分为“总体”、“网络安全支持与促进”、“网络运行安全一般规定”、“关键信息基础设施运行安全”、“个人信息保护与互联网信息内容安全”、“监测预警与应急处置”、“其他”共七部分。此外，还在附录中提供了为配合《网络安全法》实施而制定的有关政策文件的最新版（含征求意见稿）。

图书在版编目（CIP）数据

中华人民共和国网络安全法百问百答 / 左晓栋主编. — 北京：电子工业出版社，2017.8
ISBN 978-7-121-32222-8

Ⅰ. ①中… Ⅱ. ①左… Ⅲ. ①计算机网络－科学技术管理法规－中国－问题解答
Ⅳ. ①D922.170.4

中国版本图书馆CIP数据核字（2017）第167779号

策划编辑：戴晨辰
责任编辑：戴晨辰
印　　刷：
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　邮编：100036
开　　本：720×1000　1/16　印张：10.75　字数：168千字
版　　次：2017年8月第1版
印　　次：2017年8月第1次印刷
定　　价：35.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店缺售，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

本书咨询联系方式：dcc@phei.com.cn。

编写组

WRITING GROUP

左晓栋　　伍　扬

张　恒　　王政坤

前言 PREFACE

《中华人民共和国网络安全法》（本书简称《网络安全法》）已于2017年6月1日正式施行。这是我国网络安全领域的“基本法”，具有里程碑式的重大意义。《网络安全法》的起草坚持问题导向，主要针对实践中存在的突出问题，将近年来一些成熟的好做法作为制度确定下来，为网络安全工作提供切实法律保障。但同时，还有一些制度安排确有必要，但尚缺乏实践经验，《网络安全法》对此进行了原则性规定，为需要制定的配套法规政策预留了接口。在法的施行过程中，无论是国外还是国内，大家都很关心，一些条款的要求如何理解、如何落地？相关的“规定”是什么？“有关部门”是指哪里？如此等等。为此，本书总结了《网络安全法》发布以来的国内外主要关切和社会普遍关心的100个问题，并有针对性地进行了回答。书后还附上了相关部门为落实《网络安全法》而制定的有关政策文件，如《网络产品和服务安全审查办法》、《国家网络安全事件应急预案》等。对一些仍在制定中的政策，本书附上了征求意见稿，如《关键信息基础设施安全保护条例》、《重要数据识别指南》等。本书力求突出实用性，希望为各方面宣贯和施行《网络安全法》提供便利。

需要指出，编写这本百问百答，出自国家网信部门的提议，但对100个问题的梳理和回答，则是站在专家个人的角度，不代表最终的官方决策。由于编者水平有限，不妥之处在所难免，仅供读者参考。

编　者

二〇一七年七月

目 录
CONTENTS

第二部分
网络安全支持与促进

第三部分

网络运行安全一般规定

第四部分
关键信息基础设施运行安全

第一部分

PART 1 总 体

1 为什么制定《网络安全法》？

当前，网络和信息技术迅猛发展，已经深度融入我国经济社会的各个方面，极大地改变和影响着人们的社会活动和生活方式，在促进技术创新、经济发展、文化繁荣、社会进步的同时，网络安全问题也日益凸显。一是，网络入侵、网络攻击等非法活动，严重威胁着电信、能源、交通、金融，以及国防军事、行政管理等重要领域的信息基础设施的安全，云计算、大数据、物联网等新技术、新应用面临着更为复杂的网络安全环境；二是，非法获取、泄露甚至倒卖公民个人信息，侮辱诽谤他人、侵犯知识产权等违法活动在网络上时有发生，严重损害公民、法人和其他组织的合法权益；三是，宣扬恐怖主义、极端主义，煽动颠覆国家政权、推翻社会主义制度，以及淫秽色情等违法信息，借助网络传播、扩散，严重危害国家安全和社会公共利益。

党的十八大以来，以习近平同志为核心的党中央从总体国家安全观出发，就网络安全问题提出了一系列新思想、新观点、新论断，对加强国家网络安全工作作出重要部署。党的十八届四中全会决定要求完善网络安全保护方面的法律法规。广大人民群众十分关注网络安全，强烈要求依法加强网络空间治理，规范网络信息传播秩序，惩治网络违法犯罪，使网络空间清朗起来。全国人大代表也提出许多议案、建议，呼吁出台网络安全相关立法。为适应国家网络安全工作的新形势新任务，落实党中央的要求，回应人民群众的期待，制定出台了《网络安全法》。

2 制定《网络安全法》的指导思想和原则是什么？

制定《网络安全法》的指导思想是：坚持以总体国家安全观为指导，全面落实党的十八大和十八届三中、四中全会决策部署，坚持积极利用、科学发展、依法管理、确保安全的方针，充分发挥立法的引领和推动作用，针对当前我国网络安全领域的突出问题，以制度建设提高国家网络安全保障能力，掌握网络空间治理和规则制定方面的主动权，切实维护国家网络空间主权、安全和发展利益。

制定《网络安全法》把握了以下几点原则。

第一，坚持从国情出发。根据我国网络安全面临的严峻形势和网络立法的现状，充分总结近年来网络安全工作经验，确立保障网络安全的基本制度框架。重点对网络自身的安全作出制度性安排，同时在信息内容方面也作出相应的规范性规定，从网络设备设施安全、网络运行安全、网络数据安全、网络信息安全等方面建立和完善相关制度，体现中国特色。同时，注意借鉴有关国家的经验，主要制度与国外通行做法是一致的，并对内外资企业同等对待，不实行差别待遇。

第二，坚持问题导向。《网络安全法》是网络安全管理方面的基础性法律，主要针对实践中存在的突出问题，将近年来一些成熟的好做法作为制度确定下来，为网络安全工作提供切实法律保障。对一些确有必要但尚缺乏实践经验的制度安排作出原则性规定，同时注重与已有的相关法律法规相衔接，并为需要制定的配套法规预留接口。

第三，坚持网络安全与信息化发展并重。网络安全和信息化是一体之两翼，驱动之双轮。维护网络安全，必须处理好与信息化发展的关系，坚持以安全保发展、以发展促安全的要求，通过保障安全为发展提供良好环境。本法注重对网络安全制度作出规范的同时，注意保护各类网络主体的合法权利，保障网络信息依法、有序、自由流动，促进网络技术创新和信息化持续健康发展。

3 如何理解“网络安全”？

伴随信息革命的飞速发展，互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成的网络空间，正在全面改变着人们的生产生活方式，深刻影响着人类社会历史发展进程。当前，网络空间已经成为信息传播的新渠道、生产生活的新空间、经济发展的新引擎、文化繁荣的新载体、社会治理的新平台、交流合作的新纽带、国家主权的新疆域。

“网络安全”是“网络空间安全”的简称，不是“network”的安全，而是“cyber”或“cyberspace”的安全。网络安全涵盖传统意义上的信息安全、互联网安全、通

信安全、计算机安全等方面，包括互联网、通信网、计算机系统、自动化控制系统安全，同时包括这些网络和系统承载的应用、数据和信息内容的安全。

4 网络空间主权的内涵是什么？

第一条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

国家网络空间主权主要包含以下四方面内容：

一是各国根据本国国情，借鉴国际经验，制定本国有关网络空间的法律法规；

二是各国根据本国法律法规，管理本国网络空间；

三是采取必要措施，监测、保护、抵御来自国内外的网络空间威胁和攻击；

四是依法防范、阻止违法信息在本国网络空间的传播。

5 外企、驻华机构的网络是否适用本法？

第二条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

根据《网络安全法》第二条，外企和驻华机构的网络如果在中华人民共和国境内，则适用于本法。

但外国驻中国使领馆、享有外交特权的国际组织驻华机构的网络，遵照《中华人民共和国领事特权与豁免条例》等外事相关规定执行。

6 如何理解网络安全与信息化发展并重?

第三条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

中央网络安全和信息化领导小组第一次全体会议指出，网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。做好网络安全和信息化工作，要处理好安全和发展的关系，做到协调一致、齐头并进，以安全保发展、以发展促安全，努力建久安之势、成长治之业。

“以安全保发展、以发展促安全”的要求，充分体现了马克思主义的辩证法，体现了科学的发展观。网络安全是信息化推进中出现的新问题，只能在发展的过程中用发展的方式加以解决。没有网络安全，信息化发展越快，造成的危害就可能越大。而没有信息化发展，经济社会发展将会滞后，网络安全也没有保障，甚至已有的安全也会丧失。

不发展是最大的不安全。不能简单地通过不上网、不共享、不互联互通来保安全，或者片面强调建专网。这样做的结果只能是造成不必要的重复建设，大量网络资源得不到充分利用，增加信息化的成本，降低信息化效益，失去发展机遇。要以改革的精神、开放的理念、创新的机制来科学治理和化解信息化发展中出现的问题与风险，掌握国家网络空间安全战略主动权，维护网络空间安全，促进国家发展。

7 什么是国家网络安全战略？

第四条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

国家网络安全战略是为实现国家网络安全总目标而制定的总体方略，是国家网络空间安全领域的顶层设计。《网络安全法》第四条明确“国家制定并不断完善网络安全战略”。

经中央网络安全和信息化领导小组同意，国家互联网信息办公室于2016年12月公开发布了《国家网络空间安全战略》（以下简称《战略》）。《战略》阐明了中国关于网络空间发展和安全的重大立场和主张，明确了战略方针和主要任务，是指导国家网络安全工作的纲领性文件。


《国家网络空间安全战略》

《战略》明确，当前和今后一个时期，国家网络空间安全工作的战略任务是坚定捍卫网络空间主权、坚决维护国家安全、保护关键信息基础设施、加强网络文化建设、打击网络恐怖和违法犯罪、完善网络治理体系、夯实网络安全基础、提升网络空间防护能力、强化网络空间国际合作等9个方面。

《战略》要求，以总体国家安全观为指导，贯彻落实创新、协调、绿色、开放、共享的发展理念，增强风险意识和危机意识，统筹国内、国际两个大局，统筹发展、安全两件大事，积极防御、有效应对，推进网络空间和平、安全、开放、合作、有序，维护国家主权、安全、发展利益，实现建设网络强国的战略目标。

8 如何理解国家要采取措施应对来源于境内外的网络安全风险和威胁?

第五条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

《网络安全法》第五条规定了维护网络空间主权的基本要求，是对中国网络安全立场、主张、政策的重要宣示，《网络安全法》各条中关于网络安全的制度和措施，都可以认为是这一立场的具体体现。

9 为什么立法加强网络空间国际交流与合作?

第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

网络安全是全球性挑战，没有哪个国家能够置身事外、独善其身，维护网络安全是国际社会的共同责任。维护网络空间秩序，必须坚持同舟共济、互信互利的理念，摒弃零和博弈、赢者通吃的旧观念。各国应该携手努力，共同遏制信息技术滥用，反对网络监听和网络攻击，反对网络空间军备竞赛。习近平总书记在第二届世界互联网大会上讲话指出，中国愿同各国一道，加强对话交流，有效管控分歧，推动制定各方普遍接受的网络空间国际规则，制定网络空间国际反恐公

约，健全打击网络犯罪司法协助机制，共同维护网络空间和平安全。

为此，《网络安全法》在第七条中明确，国家积极开展有关网络安全国际交流与合作，包括但不限于网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面。

2017 年 3 月 1 日，经中央网络安全和信息化领导小组批准，外交部和国家互联网信息办公室共同发布《网络空间国际合作战略》。战略以和平发展、合作共赢为主题，以构建网络空间命运共同体为目标，就推动网络空间国际交流合作，首次全面系统提出中国主张，为破解全球网络空间治理难题贡献中国方案，是指导中国参与网络空间国际交流与合作的战略性文件。


《网络空间国际合作战略》

10 如何理解“和平、安全、开放、合作”的网络空间?

第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

和平，指信息技术滥用得到有效遏制，网络空间军备竞赛等威胁国际和平的活动得到有效控制，网络空间冲突得到有效防范。

安全，指网络安全风险得到有效控制，国家网络安全保障体系健全完善，核心技术装备安全可控，网络和信息系统运行稳定可靠。网络安全人才满足需求，全社会的网络安全意识、基本防护技能和利用网络的信心大幅提升。

开放，指信息技术标准、政策和市场开放、透明，产品流通和信息传播更加顺畅，数字鸿沟日益弥合；不分大小、强弱、贫富，世界各国特别是发展中国家都能分享发展机遇、共享发展成果、公平参与网络空间治理。

合作，指世界各国在技术交流、打击网络恐怖和网络犯罪等领域的合作更加密切，多边、民主、透明的国际互联网治理体系健全完善，以合作共赢为核心的网络空间命运共同体逐步形成。

11 如何理解“多边、民主、透明”的网络治理体系？

第七条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

中国主张通过国际社会平等参与和共同决策，构建多边、民主、透明的全球互联网治理体系。“多边”实质是，国家不分大小、强弱、贫富，都是国际社会平等成员，都享有平等参与互联网治理的权利。与中国提出的互联网治理模式相对应的，是一些西方国家所主张的“多利益攸关方”模式。《网络安全法》强调“多边、民主、透明”，但并不否认“多方”模式及“多方”的重要作用。中国支持加强包括各国政府、国际组织、互联网企业、技术社群、民间机构、公民个人等各利益攸关方的沟通与合作。关键是，各利益攸关方应在“多方”治理模式中发挥与自身角色相匹配的作用，政府应在互联网治理特别是公共政策和安全中发挥关键主导作用，实现共同参与、科学管理、民主决策。

“民主、透明”的内涵是，应公平分配互联网基础资源，共同管理互联网根服务器等关键信息基础设施，要确保相关国际进程的包容与开放，加强发展中国家的代表性和发言权。

12 如何理解国家网信部门负责统筹协调网络安全工作?

第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

《网络安全法》明确国家网信部门统筹协调国家网络安全工作，主要是网络安全政策、信息、资源、事件处置的统筹协调，重点包括以下四方面。

一是《网络安全法》明确的统筹协调工作，包括：第三十九条规定的协调有关部门加强对关键信息基础设施的安全保护；第五十一条规定的协调有关部门加强网络安全信息收集、分析和通报工作，按照统一规定发布网络安全监测预警信息；第五十三条规定的协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

二是根据部门职能和中央的要求，应该承担的统筹协调工作，包括：组织拟订国家网络安全战略、规划等；统筹协调国家网络安全保障体系和可信体系建设；组织起草关键信息基础设施保护条例、数据安全保护办法等；指导组织国家网络安全标准的制定；指导督促党政军部门、重点行业网络安全保障工作；推进网络安全人才培养工作等。

三是《网络安全法》中有些工作任务未明确责任主体的，应该通过统筹协调进一步推进，如国家支持研究开发有利于未成年人健康成长的网络产品和服务；国务院和各地方人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目等。

四是《网络安全法》中多次提到了“按规定”但目前还没有规定的事项。对于没有规定的或规定不完善的，要统筹协调、抓紧制定和完善相关规定。

13 如何理解国家网信部门负责网络安全相关监督管理工作?

第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

一是《网络安全法》中明确了由国家网信部门承担的管理工作，主要包括：① 受理和处置网络安全举报；② 对出境数据组织安全评估；③ 对可能影响国家安全的产品和服务组织网络安全审查；④ 制定网络关键设备和网络安全专用产品目录；⑤ 发现法律法规禁止发布或者传输的信息时，应当要求网络运营者停止传输；⑥ 对来源于境外的违法信息，通知有关机构采取技术措施和其他必要措施，阻断传播。

二是根据国家有关要求，明确了由网信部门为主承担的网络安全工作，包括：① 具体承担网络内容安全管理工作；② 组织开展网络安全宣传教育活动等。

三是《网络安全法》中虽未明确具体部门，但有关规定在实施时实际由网信部门为主，承担工作。如第五十二条规定，负责关键信息基础设施安全保护工作的部门，应当按照规定报送网络安全监测预警信息，这里要求的信息应向网络安全应急办所在的网信部门报送。

14 《网络安全法》规定的县级以上人民政府有关部门的网络安全保护和监督管理职责如何落实？

第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

根据有关精神，各省级网信部门作为本地区网络安全统筹协调部门，应当设立专门的网络安全机构，培养网络安全支撑机构。地（市）、县两级也应建立网络安全专门工作机构，或者明确相关部门负责网络安全工作，承担相应责任。

15 《网络安全法》明确规定的地方政府的网络安全责任有哪些？

第八条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

一是按照第十六条要求，统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，

保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

二是按照第十九条要求，组织开展经常性的网络安全宣传教育，指导、监督有关单位做好网络安全宣传教育工作。

三是按照第五十四条要求，网络安全事件发生的风险增大时，应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取以下措施：① 要求有关部门、机构和人员及时收集、报告有关信息，加强网络安全风险的监测；② 组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；③ 向社会发布网络安全风险预警，发布避免、减轻危害的措施。

四是按照第五十五条要求，发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

五是按照第五十六条要求，在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序，对该网络运营者的法定代表人或者主要责任人进行约谈。

六是按照第十四条要求，建立网络安全举报受理机制。

七是按照第四十九条要求，依法对网络运营者实施监督检查。

16 《网络安全法》规定的网络运营者应该承担的责任，是否适用于个人、家庭及所有企业和机构？

第九条 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

《网络安全法》第九条规定，“网络运营者开展经营和服务活动，必须遵守法律、行政法规”。以后法律各条中关于网络运营者的责任都是指网络运营者在开展网络经营和服务过程中所必须遵守的。如果不开展经营或网络服务活动，就不适用这些要求。

17 为什么鼓励网络相关行业组织制定网络安全行为规范?

第十一条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

我国的网络治理体系具有法律规范、行政监管、行业自律、技术保障、公众监督、社会教育相结合的特点。其中，行业自律是重要一环。

《网络安全法》第十一条规定，网络相关行业组织制定网络安全行为规范。一方面，规范具有指导作用，可促进会员加强自身网络安全保护；另一方面，规范具有约束作用，可规范行业行为，保护用户权益。这是维护网络安全、促进全行业健康发展的重要措施。

行业组织在制定网络安全行为规范时，应坚持公开、公正、公平的原则，充分听取行业内外相关方的意见。

18 《网络安全法》对个人和组织提出了哪些明确的行为禁则?

《网络安全法》明确禁止了八类活动、七种行为。

任何个人和组织不得利用网络从事以下八类活动：一是危害国家安全、荣誉

和利益的活动；二是煽动颠覆国家政权、推翻社会主义制度的活动；三是煽动分裂国家、破坏国家统一的活动；四是宣扬恐怖主义、极端主义的活动；五是宣扬民族仇恨、民族歧视的活动；六是传播暴力、淫秽色情信息的活动；七是编造、传播虚假信息扰乱经济秩序和社会秩序的活动；八是侵害他人名誉、隐私、知识产权和其他合法权益的活动。

以下七种行为都是法律明确禁止的：一是非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；二是提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；三是明知他人从事危害网络安全的活动，仍为其提供技术支持、广告推广、支付结算等帮助；四是窃取或者以其他非法方式获取个人信息，非法出售或者非法向他人提供个人信息；五是设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组；六是利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品，以及其他违法犯罪活动的信息；七是发送的电子信息、提供的应用软件，设置了恶意程序，含有法律、行政法规禁止发布或者传输的信息。

19 如何加强对未成年人的网络保护？

第十三条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

《网络安全法》注重保护未成年人上网安全，营造有利于未成年人健康成长的网络环境。第十三条对此作了专门规定。

2017 年 1 月 6 日，国务院法制办公布了《未成年人网络保护条例（送审稿）》

及其说明，向社会各界征求意见。送审稿落实《网络安全法》要求，针对网络信息内容建设、未成年人网络权益保障、预防和干预、法律责任等方面作出了详细规定。

20 个人和组织对危害网络安全的行为如何举报？

第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

任何个人和组织发现危害网络安全的八类活动、七种行为时，都有权举报。原则上讲，涉及网络犯罪的主要是向公安部门举报，其他类型的，既可以向电信部门，也可以向网信等部门举报。但是，无论是哪一类危害网络安全的行为，个人和组织都可以向网信、电信、公安等部门举报。

任何一个部门收到举报都应该及时处理，不属于本部门职责的要及时移交相关部门处理。

21 《网络安全法》是否会限制国外技术和产品？

习近平总书记强调：“我们不拒绝任何新技术，新技术是人类文明发展的成果，只要有利于提高我国社会生产力水平、有利于改善人民生活，我们都不拒绝。”《网络安全法》贯彻习近平总书记的指示精神，是一部促进发展和开放的法律，坚持以安全保发展，以发展促安全，立足全球化和互联互通的开放环境维护网络安全，

支持而不是限制国际合作。

中国过去没有，现在也没有，将来也不会以网络安全为由闭关锁国。只要各国企业切实遵守中国法律法规，都欢迎他们同中国企业共同研究、共同制造、共同发展。

22 是否会根据《网络安全法》的规定，要求企业向中国政府提供产品源代码？

中国高度重视知识产权保护，不会以网络安全为由要求企业将源代码交给政府部门。一些境外媒体、外国行业组织针对源代码问题对《网络安全法》的指责没有事实依据。

23 《网络安全法》对网络运营者规定了哪些责任、义务？

《网络安全法》规定的网络运营者责任、义务主要包括：

一是第二十一条关于网络安全等级保护五方面的要求，即：制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；采取数据分类、重要数据备份和加密等措施；法律、行政法规规定的其他义务。

二是第二十二条关于网络运营者提供产品、服务时的要求，即：如果网络运营者对外提供产品和服务，则应当符合相关国家标准的强制性要求。具体是：不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。网络产品、服务具有收集用户信息功能的，其提

供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

三是第二十四条关于实名制的要求，即：网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

四是第二十五条关于网络安全事件处置的要求，即：网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

五是第二十八条关于提供技术支持和协助的要求，即：网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

六是第四十条、第四十一条、第四十二条、第四十三条关于用户和个人信息保护的要求。

七是第四十七条关于信息发布的要求，即：网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

八是第四十九条关于投诉举报和配合网信等部门实施安全检查的要求，即：网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

24 《网络安全法》对关键信息基础设施运营者规定了哪些责任、义务？

关键信息基础设施运营者除了履行网络运营者的责任、义务外，还应履行以下责任、义务。

一是第三十三条关于“三同步”的要求，即：建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

二是第三十四条提出的设置专门安全管理机构、培训等五方面要求，即：设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；定期对从业人员进行网络安全教育、技术培训和技能考核；对重要系统和数据库进行容灾备份；制定网络安全事件应急预案，并定期进行演练；法律、行政法规规定的其他义务。

三是第三十五条关于国家网络安全审查要求，即：关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

四是第三十六条关于签订安全保密协议的要求，即：关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

五是第三十七条关于数据出境的要求，即：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。

六是第三十八条关于每年开展安全检测评估的要求，即：关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第二部分

PART 2

网络安全支持与促进

25 如何加强国家网络安全标准体系建设?

第十五条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

网络安全标准化是网络安全保障体系建设的重要组成部分，在构建安全的网络空间、推动网络治理体系变革方面发挥着基础性、规范性、引领性作用。《网络安全法》不但提出了建立和完善网络安全标准体系的要求，而且多次强调网络安全工作应该符合国家标准的强制性要求，进一步提升了网络安全标准的地位和作用。

全国信息安全标准化技术委员会（TC260）以制定国家网络安全保障体系建设亟需的、关键的标准为重点，积极开展标准制定和修订工作，基本形成了我国网络安全标准体系，为我国网络安全保障体系建设提供了强有力的支持。随着信息技术的快速发展，新技术、新应用的网络安全标准相继制定，我国的网络安全标准体系将日趋完善。

2016 年，经中央网络安全和信息化领导小组同意，中央网信办、国家质检总局、国家标准委联合印发了《关于加强国家网络安全标准化工作的若干意见》，要求建立统筹协调、分工协作的工作机制，加强标准体系建设，提升标准质量和基础能力，强化标准宣传实施，加强国际标准化工作，抓好标准化人才队伍建设，以及做好资金保障。根据该意见，全国

《关于加强国家网络安全标准化工作的若干意见》

信息安全标准化技术委员会在国家标准委的领导下，在中央网信办的统筹协调和有关网络安全主管部门的支持下，对网络安全国家标准进行统一技术归口，统一组织申报、送审和报批。全国信息安全标准化技术委员会在业务上受中央网信办指导。

26 外国企业能否参与制定行业和国家网络安全标准？

一直以来，中国高度重视网络安全标准的国际交流与合作，积极参与国际网络安全标准化活动，发挥建设性作用。

中国也欢迎外国企业参与网络安全标准化工作。根据全国信息安全标准化技术委员会工作组章程规定，在中国境内注册的、具有法人资格的企业、高等院校、科研院所（不包含协会）是成为工作组成员应具备的基本条件。只要是在中国境内注册，具有法人资格的境外企业，自愿加入全国信息安全标准化技术委员会工作组，承认并遵守《全国信息安全标准化技术委员会工作组章程》，且从事与工作组技术领域相关的业务，就可以申请成为工作组成员单位，经工作组审批通过后，即可参与国家网络安全标准的制定工作。目前，有近 20 家外国企业参加了该委员会下属的各个工作组。

除工作组外，全国信息安全标准化技术委员会的委员资格也是对外企开放的。目前，全国信息安全标准化技术委员会有委员 81 人，其中有 4 位委员来自外国企业。

中国在网络安全标准化工作中，十分注重同国际标准相衔接，在已出台的接近 200 项国家网络安全标准中，有不少都是等同采用国际标准。

27 “安全可信”的网络产品和服务是什么含义？

第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

安全可信与自主可控、安全可控有着相同的基本要求，主要包括三方面：

一是产品或服务提供者不应利用提供产品或服务的便利条件非法获取用户重要数据，损害用户对自己数据的支配权；

二是产品或服务提供者不应通过网络非法控制和操纵用户设备，损害用户对自己所拥有和使用设备的控制权；

三是产品和服务提供者不应利用用户对产品和服务的依赖性牟取不正当利益，实施垄断经营，包括停止提供合理的安全技术支持，迫使用户更新换代。

提出安全可信的要求主要是为了保障用户利益，无论是国外产品还是国内产品，都应该符合安全可信的要求，不得损害用户利益。

28 为什么要鼓励开发网络数据安全保护和利用技术？

第十八条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

数据是国家基础性战略资源，开发网络数据安全保护和利用技术，对加强数据安全保护，充分发挥数据价值，促进经济社会健康发展有重要意义。

网络数据具有体量大、结构多样、处理迅速、价值高等特性。随着信息技术的快速发展，传统的数据安全保护技术不再适用于当前数据环境，数据不能有效利用、数据安全得不到保障等问题日益突出，网络数据安全保护和利用技术越来越重要。

开发网络数据安全保护和利用技术，是保护数据安全、充分挖掘和利用数据价值的关键，也是维护网络安全和国家安全，以及推动国家大数据产业发展的需要。目前，各国都高度重视数据安全保护和利用技术，很多国家在这方面采取了鼓励措施。

29 如何理解创新网络安全管理方式，运用网络新技术，提升网络安全保护水平？

第十八条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

随着互联网技术的发展，相关网络产品和服务的技术架构、业务形态快速迭代、演进，数据规模急速膨胀，产品和服务的提供形式、与用户的交互方式也不断变化，新的技术和业务形态带来新的安全挑战，需要构建与之协调发展的网络安全管理方式，积极创新并利用新的技术维护和提升网络安全保护水平。

特别是，为了落实“以安全保发展、以发展促安全”的要求，不能以断开网络、停止应用等牺牲信息化发展的消极方式保安全，而应当积极利用信息化发展的成果，特别是新的网络技术保障安全。大数据时代的到来为保障网络安全提供了新

的思路。习近平总书记要求，应发挥 1+1 大于 2 的效应，以综合运用各方面掌握的数据资源，加强大数据挖掘分析，更好感知网络安全态势，做好风险防范。

30 国家如何开展经常性的网络安全宣传教育活动？

第十九条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

网络安全是共同的而不是孤立的。网络安全为人民，网络安全靠人民，维护网络安全是全社会共同责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。

自 2014 年起，国家设立了网络安全宣传周，前两届均在北京举办。2016 年 3 月，经中央网络安全和信息化领导小组同意，中央网信办、教育部、工业和信息化部、公安部、国家新闻出版广电总局、共青团中央联合印发了《国家网络安全宣传周活动方案》，规定网络安全宣传周统一于每年 9 月份第 3 周举办，宣传周中的开幕式等重要活动，可根据地方实际情况安排在省会城市举行。通过在全国范围内集中开展网络安全宣传教育活动，网络安全周旨在增强广大网民的网络安全意识，提升基本防护技能，营造安全、健康、文明的网络环境，保障人民群众在网络空间的合法权益，切实维护国家网络安全。

31 国家如何支持网络安全相关教育与培训活动?

第二十条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

网络空间的竞争，归根结底是人才竞争。从总体上看，我国网络安全人才还存在数量缺口较大、能力素质不高、结构不尽合理等问题，与维护国家网络安全、建设网络强国的要求不相适应。习近平总书记在 2016 年 4 月 19 日召开的网络安全和信息化工作座谈会上指出，要下大功夫、下大本钱，请优秀的老师，编优秀的教材，招优秀的学生，建一流的网络空间安全学院。

为加强网络安全学院学科专业建设和人才培养，经中央网络安全和信息化领导小组同意，中央网信办、发展改革委、教育部、科技部、工业和信息化部、人社部等六部委于 2016 年 6 月联合印发了《关于加强网络安全学科建设和人才培养的意见》。文件提出，要加快网络安全学科专业和院系建设，创新网络安全人才培养机制，加强网络安全教材建设，强化网络安全师资队伍建设，推动高等院校与行业企业合作育人、协同创新，加强网络安全从业人员在职培训，完善网络安全人才培养配套措施。文件要求，各地方、各部门要认识到网络安全学科建设和人才培养的极端重要性，增强责任感、使命感，将网络安全人才培养工作提到重要议事日程，并结合实际制定具体措施，支持网络安全学院学科专业建设，加快网络安全人才培养，为实施网络强国战略、维护国家网络安全提供强大的人才保障。

《关于加强网络安全学科建设和人才培养的意见》

第三部分

PART 3

网络运行安全一般规定

32 网络安全等级保护制度与现行的信息安全等级保护制度是什么关系?

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

信息安全等级保护是国家网络安全保障的重要制度，其核心是分清系统边界，明确系统责任，确保重点目标的安全。近年来，信息安全等级保护制度在国家网络安全保障中发挥了重要作用，但该制度也应随着形势的发展不断完善，如云计算、大数据、物联网、移动互联网等技术的发展，使系统边界日益模糊，迫切需要从整体上加强保护。《网络安全法》提出了“实行网络安全等级保护制度”，明确了网络安全等级保护制度的基本要求，这是在总结信息安全等级保护工作的基础上，根据网络安全的新形势、新特点提出的，标志着信息安全保护制度进入了一个新的阶段。

33 什么样的设备和系统应当留存网络日志不少于六个月？

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

《网络安全法》第二十一条要求，网络运营者应按照规定留存相关的网络日志不少于六个月。这里的网络日志主要是指记录网络运行和安全状况、网络行为等的文件，一般不包括个人终端上的日志文件。

34 什么是国家标准的强制性要求？

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知

用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

强制性标准是在一定范围内通过法律、行政法规等强制性手段加以实施的标准，具有法律属性，强制性标准可分为全文强制和条文强制两种形式。今后，按照标准化改革方案要求，国家标准的强制性要求，主要是指强制性国家标准。

目前，我国已经出台的国家网络安全标准，基本上为指导性标准。全国信息安全标准化技术委员会将按照《网络安全法》的要求和网络安全工作需要，从维护国家安全、用户利益出发，对网络产品、服务制定强制性国家网络安全标准。

35 网络产品、服务存在安全缺陷、漏洞等风险时，应如何告知用户并向有关主管部门报告？

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

针对近年来网络产品、服务存在缺陷、漏洞并被恶意利用，损害用户利益的情况，《网络安全法》强化了用户知情权。有关产品和服务的提供者应在避免安全缺陷与漏洞被进一步利用的前提下，选择通过电话、短信、邮件、网站公告、媒体广告等合理方式告知用户，并提供相应的风险解决或减轻措施。此外，网络产品、服务提供者应当根据产品、服务的主要使用领域、事件性质等，向网信、电信、公安等部门报告。

36 如何理解网络产品、服务的提供者应当持续提供安全维护？

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

《网络安全法》第二十二条规定，网络产品、服务提供者应当为其产品、服务持续提供安全维护，这里的“持续”是指在规定或者当事人约定的期限内不得终止提供安全维护。特别是，网络产品、服务提供者不得利用用户对产品和服务的依赖，损害用户利益。

37 什么是“网络关键设备”和“网络安全专用产品”？

第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

网络关键设备是指接入到面向公众提供服务的网络系统、国家基础网络或行业业务网络系统，并对其服务提供或业务运行具有重要支撑作用的实体（包括虚拟化功能的实体）。这些实体一旦遭受攻击、发生故障可能严重影响网络运行，导致大量数据泄露，将对国家政治、经济、科技、社会、文化、环境及人民生命、财产造成严重损失，实体如高端路由器、交换机等。

网络安全专用产品是指专门用于防范对网络的攻击、侵入、干扰、破坏和非法使用及意外事故，使网络处于稳定可靠、可控运行的状态，以及保障网络数据的完整性、保密性、可用性的信息技术软件、硬件及其组合体，如加密机、防火墙、入侵检测系统等专门提供网络安全防护功能的产品。

国家网信部门会同有关部门制定了《网络关键设备和网络安全专用产品目录（第一批）》，对网络关键设备和网络安全专用产品作出了具体规定。首批目录中，网络关键设备包括 4 类，网络安全专用产品包括 15 类。该目录将保持适时更新。

38 在进行安全认证或安全检测时，什么是“具备资格的机构”？

第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

具备资格的机构指国家认证认可监督管理委员会、工业和信息化部、公安部、国家互联网信息办公室按照国家有关规定共同认定的机构。国家网信部门会同有关部门正在制定网络关键设备和网络安全专用产品认证检测机构资格条件和认定办法。

39 外国人员携带设备进入中国是否需要检测和认证？

《网络安全法》中关于网络关键设备和网络安全专用产品的安全认证和安全检测要求，针对的是上述设备和产品的生产者、经营者，不包括个人使用者。

外国人员从中国境外带入境内的自用物品，或者外国政府援助、赠送的物品，一般不需要经过检测和认证。对于用于科研、测试、展示等非自用用途的物品，应按规定取得免予检测、认证证明后，方可携带入境。

40 如何理解第二十三条的强制性市场准入要求？

第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

同时具备以下两种条件的产品，应当按照《网络安全法》第二十三条规定进行认证检测，否则不可销售或者提供：一是列入《网络关键设备和网络安全专用产品目录》的产品，二是国家标准有相关强制性要求的产品。

在目录内的产品，且国家标准有相关强制性要求的，如果有关部门在《网络安全法》实施前已按要求对其进行了认证检测，在有效期内无须再进行认证检测。

41 我国是否认可国外认证和检测机构的认证及检测结果？

任何机构，只要具备网络关键设备和网络安全专用产品认证检测机构资格条件和认定办法的相应资格，就可以参与对网络关键设备和网络安全专用产品的认证和检测工作。

中国重视网络安全认证认可领域的国际交流合作，有关部门正在就网络安全国际互认问题进行研究。

42 如何理解《网络安全法》对提供用户真实身份信息所作的要求？

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

《网络安全法》第二十四条规定，应在三种情况下要求用户提供真实身份信息：一是办理网络接入、域名注册服务；二是办理固定电话、移动电话等入网手续；三是为用户提供信息发布、即时通讯等服务。这是为了更好地维护网络秩序，追踪和打击各类网络违法犯罪行为，也是构建网络可信环境、促进网络发展的重要手段。

当前，在保障公民合法权益、查处网络违法犯罪过程中，因网络行为主体身份信息不清楚，导致许多违法犯罪活动没有得到及时查处，公民合法权益没有得到有效维护，迫切需要通过加强网络空间身份管理来打击网络违法犯罪行为，维护人民群众合法权益。

根据立法的指导思想，网络运营者收集的用户真实身份信息只能用于维护国家网络安全，不能用于其他目的。

需要指出，《网络安全法》第二十四条规定的实名制，并不是指用户使用互联网的任何行为必须实名，而是要求在互联网上从事信息发布、即时通讯等活动时应当实名。

43 网络运营者在提供信息发布、即时通讯服务时验证用户真实身份信息在技术和成本上是否可行？

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

在信息发布、即时通讯等服务中，网络运营者在线验证用户身份证有时会面临困难。但查验用户真实身份信息的途径和方法多种多样，并不仅限于验证用户的身份证。例如，在全面落实手机实名制的前提下，通过发送注册码的方式验证用户手机就是一个高效、可行的办法，同时可以确保用户真实身份的匿名。随着网络空间身份管理体系建设的推进，会有越来越多便捷、可靠的方法用于验证用户真实身份，这些方法对网络运营者不会带来负担。

44 用户提供真实身份信息是否会影响个人隐私？

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

中国致力于促进互联网的发展，依法保护公民在互联网上的言论自由，保障公众的知情权、参与权、表达权、监督权。《网络安全法》在反恐法确立的电信用户实名制基础上，规定了信息发布、即时通讯等服务的实名制要求，这样的要求同依法保障言论自由并不矛盾。

《网络安全法》要求用户提供真实身份信息，并不意味着用户在网上发言必须使用实名信息，用户可以使用网名或匿名，从而实现“前台自愿、后台实名”。

在要求用户提交真实身份的同时，《网络安全法》也对包括用户身份信息在内的个人信息保护提出了严格的要求，既能满足监管和打击犯罪的需要，又充分保障了用户权益。

45 什么是网络可信身份战略？

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

信任是社会互动的桥梁，是社会建设与发展的基础。随着网络空间的发展，贸易、购物、交友、培训、会谈、娱乐等越来越多的社会活动由现实世界迁移到网络空间中进行，因此对网络空间信任体系的建立提出了迫切需要。

建立网络空间信任体系，首先需要解决网络行为主体的身份可信问题。这里的网络行为主体既包括自然人，也包括企业组织、网络设备、终端设备、软件、服务等网络中存在的非自然人实体。网络可信身份战略，就是从法律、政策、规则、技术等方面着手确定网络主体身份、属性、信用等，并通过网络权限管理、行为追溯、责任认定等技术，建立可信的网络环境，服务社会治理、经济发展和安全保护。

目前，国家网信部门正在会同有关部门研究制定网络可信身份战略。

46 发生危害网络安全的事件时，网络运营者应如何报告？

第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

国家网信部门已经发布了《国家网络安全事件应急预案》，网络运营者应根据国家预案，制定本单位的网络安全事件应急预案。在发生危害网络安全的事件时，网络运营者应立即启动应急预案，采取补救措施，按照《国家网络安全事件应急预案》规定的报告程序进行报告。

47 如何理解开展网络安全认证、向社会发布网络安全信息等应当遵守国家有关规定？

第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

开展网络安全认证、向社会发布网络安全信息等对行业和社会影响较大，对这类服务应该进行规范。特别是，一些组织和个人未经产品和服务提供者同意，随意公开产品和服务的安全缺陷、漏洞，甚至攻击方法、漏洞利用方法，带来很大安全风险；有的企业和机构擅自发布网络安全攻击、事件后果等信息，夸大危害和影响，甚至引发社会恐慌。因此，在发布此类信息时，应当确保发布信息的权威性、准确性，防止被恶意利用，应维护行业秩序，保护有关方面的合法权益。

开展网络安全认证活动，应符合《认证认可条例》，符合网络关键设备和网络安全专用产品认证检测机构资格条件和认定办法及其他有关文件的规定。

此外，国家网信部门正在会同有关部门制定《网络安全威胁信息发布管理办法》，对向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息作出规定。

48 企业为公安机关、国家安全机关提供技术支持和协助，是否会损害个人隐私、侵犯知识产权？

第二十八条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

出于维护国家安全、保护公民合法权益和打击网络犯罪，特别是打击网络恐怖活动的需要，要求企业为执法部门提供必要的支持和协助是各国的通行做法，也是企业应尽的义务。

《网络安全法》规定，相关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途，并明确规定相关部门及其工作人员不得泄露、出售或者非法向他人提供在履行职责中知悉的个人信息、隐私和商业秘密。在实际执行过程中，对执法部门也会有约束，执法部门要履行严格的审批程序，最大限度地降低可能对企业造成的影响。

49 为什么强调网络运营者之间的网络安全合作？

第二十九条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

当前，曾经分散独立的网络变得高度关联、相互依赖，网络安全的威胁来源和攻击手段不断变化，“单打独斗”的时代已经过去，依靠装几个安全设备和安全软件就想永保安全的想法也已不合时宜，网络运营者需要树立动态、综合的防护理念。为此，《网络安全法》鼓励网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，形成合力。《网络安全法》还强调发挥行业组织的作用，建立健全本行业的网络安全保护规范和协作机制，且行业组织要为会员提供更多的专业化网络安全服务。

第四部分

PART 4

关键信息基础设施运行安全

50 关键信息基础设施的范围有哪些?

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

很多国家都通过立法等措施加强了对能源、交通、水利、通信等国家关键基础设施的网络安全保护。根据中国的实践和维护国家网络安全需要，借鉴国外经验，《网络安全法》明确对关键信息基础设施实行重点保护。同时指出，关键信息基础设施是指那些一旦遭到破坏、丧失功能或者数据泄露将对国家安全、国计民生、公共利益造成严重危害的网络设施和信息系统。

《网络安全法》要求，关键信息基础设施的具体范围和安全保护办法由国务院制定。

51 什么是“关键信息基础设施安全保护办法”?

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键

信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

根据国务院的要求，国家网信部门已会同有关部门起草了《关键信息基础设施安全保护条例》，目前正在征求意见。按程序报批后，将以国务院行政法规的形式发布。该条例明确了关键信息基础设施的具体范围，并提出了进一步的安全保护要求。

52 为什么要加强关键信息基础设施保护？

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

金融、能源、通信、交通等重点行业和领域的关键信息基础设施是经济社会运行的神经中枢，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生和公共利益。当前，关键信息基础设施是网络攻击的重点目标，其安全保护是网络安全的重中之重。面对当前严峻的网络安全形势，各国普遍加强对关键信息基础设施的保护，出台了一系列政策法规。

十八大以来，习近平总书记就切实做好国家关键信息基础设施安全保护提出明确要求，强调这些领域“不出问题则已，一出就可能导致交通中断、金融紊乱、电力瘫痪等问题，具有很大的破坏性和杀伤力”，并指示深入研究，采取有效措施，切实做好国家关键信息基础设施安全防护，加快构建关键信息基础设施安全保障体系。

53 关键信息基础设施是否包括外企在中国境内的信息系统?

《网络安全法》已经明确，在中华人民共和国境内建设、运营、维护和使用网络，适用本法。是否列为关键信息基础设施，主要看网络和信息系统遭到破坏、丧失功能或者数据泄露后，是否会严重危害中国国家安全、国计民生和公共利益，与境内的关键信息基础设施由谁所有和由谁运营没有必然联系。

54 如何理解“自愿参与关键信息基础设施保护体系”？

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

除关键信息基础设施外，还有大量的网络和信息系统在运行。这些经营与服务性的网络和信息系统的重要性、影响力比不上关键信息基础设施，但仍应满足《网络安全法》在“网络运行安全”中作出的“一般规定”。《网络安全法》及今后出台的《关键信息基础设施安全保护条例》和有关标准，对关键信息基础设施安全提出了较高要求，在成本合适的情况下，非关键信息基础设施的运营者也可以参考或落实这些要求，但这些要求对非关键信息基础设施不是强制的。

同时，自愿参与关键信息基础设施保护体系，可以扩大信息共享等合作机制的范围，使更多的网络运营者参与到网络安全风险应对、处置的过程中，扩大网络安全态势感知范围，有利于提升网络安全事件处置的协同配合能力。

55 网络安全等级保护制度与关键信息基础设施保护制度是什么关系？

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

《网络安全法》明确，关键信息基础设施保护要“在网络安全等级保护制度的基础上，实行重点保护”，指的是关键信息基础设施保护首先要满足网络安全等级保护的基本要求，主要是《网络安全法》第二十一条提出的要求，同时还要采取更加完善的措施来确保其安全。

今后，要按照《网络安全法》的要求，把关键信息基础设施保护作为网络安全工作的重中之重。一是要加强关键信息基础设施保护的统筹，加强顶层设计和整体防护，避免多头分散、各自为政的情况发生；二是要建立完善责任制，政府主要是加强指导监管，关键信息基础设施运营者要承担起保护的主体责任；三是要加强对从业人员的网络安全教育、技术培训和技能考核，切实提高网络安全意识和水平；四是要做好网络安全信息共享、应急处置等基础性工作，提升关键信息基础设施保护能力；五是要加强关键信息基础设施保护中的国际合作。

56 什么是“负责关键信息基础设施安全保护工作的部门”？

第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

各行业、各领域的主管或监管部门依据职责分工，负责本行业、本领域关键信息基础设施的安全保护工作。国家网信部门将加强对关键信息基础设施安全保护工作的统筹和指导监督。

57 为什么要求关键信息基础设施安全保护部门编制和组织实施本行业、本领域的关键信息基础设施安全规划？

第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

各行业、各领域关键信息基础设施形态各异，支撑的业务千差万别，具体到每一个行业，其保护工作的重点、保护的手段等不尽相同。各行业主管或监管部门对本行业的安全本身负有管理职责，且其对行业内关键信息基础设施情况最为了解，对业务网络安全需求最为明确。因此，由行业主管或监管部门编制和组织实施本行业、本领域的关键信息基础设施安全规划最为合理。

58 如何理解“三同步”？

第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

《网络安全法》第三十三条规定的“三同步”是强调，在信息系统的规划、设计、实施、运维、废弃的整个生命周期阶段，必须同步考虑网络安全，不能出现“有发展、无安全，有规划、无建设，有建设、无使用”等情况。具体而言，要求在信息系统生命周期的相关阶段，同步规划安全目标、设计安全措施、建设安全措施、开展安全运维，并确保系统废弃过程的安全。

59 如何对关键信息基础设施安全管理机构负责人和关键岗位的人员进行安全背景审查？

第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；
（三）对重要系统和数据库进行容灾备份；
（四）制定网络安全事件应急预案，并定期进行演练；
（五）法律、行政法规规定的其他义务。

原则上由关键信息基础设施的运营者自己组织审查，国家网信部门会同有关部门加强指导。

60 接受网络安全教育、技术培训和技能考核的从业人员包括哪些人员？

第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：
（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；
（二）定期对从业人员进行网络安全教育、技术培训和技能考核；
（三）对重要系统和数据库进行容灾备份；
（四）制定网络安全事件应急预案，并定期进行演练；
（五）法律、行政法规规定的其他义务。

当前存在很多安全隐患是因为安全意识不到位，安全操作不当造成的，例如：有的单位的重要系统用户登录口令过于简单，且长期不予以修改；有的单位虽然配备了安全防护设备，但设备的安全功能模块设置不当，不能正常发挥作用；有的单位对个人信息或其他重要数据安全管理不规范，对访问人员疏于严格限制等。因此，人的意识和技能十分重要，而网络安全意识和技能的提升主要依靠定期的

培训，而且要通过考核将培训落到实处。

《网络安全法》第三十四条中的“从业人员”不仅限于网络安全岗位上的专业人员，还包括其他与关键信息基础设施运营安全相关的管理人员、操作人员、使用人员、服务人员等，是全员教育、培训和考核。

61 如何对重要系统和数据库进行容灾备份？

第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）法律、行政法规规定的其他义务。

容灾备份是信息系统灾难恢复工作的重要组成部分。完整的灾难恢复工作包括灾难恢复规划和灾难备份中心的日常运行、关键业务功能在灾难备份中心的恢复和重续运行，以及主系统的灾后重建和回退工作，还涉及突发事件发生后的应急响应。

我国国家标准 GB/T 20988-2007《信息安全技术 信息系统灾难恢复规范》将灾难恢复能力划分为 6 个级别，由低到高逐级增强。第 1 级为“基本支持”，对网络和系统备份不作要求，完全的数据备份至少每周一次，且备份介质场外存放；第 2 级为“备用场地支持”，灾难发生后能在预定时间内调配所需的数据处理设备、通信线路和网络设备到备用场地，完全的数据备份至少每周一次，且备份介

质场外存放；第 3 级为“电子传输和部分设备支持”，配备灾难恢复所需的部分数据处理设备、部分通信线路和相应的网络设备，完全的数据备份至少每天一次，且备份介质场外存放，每天多次利用通信网络将关键数据定时批量传送至备用场地；第 4 级为“电子传输及完整设备支持”，配备灾难恢复所需的全部数据处理设备、通信线路和网络设备，并处于就绪状态或运行状态，数据备份要求同第 3 级；第 5 级为“实时数据传输及完整设备支持”，在第 4 级的基础上，具备通信网络自动或集中切换能力，并采用远程数据复制技术，利用通信网络将关键数据实时复制到备用场地；第 6 级为“数据零丢失和远程集群支持”，备用数据处理系统具备与生产数据处理系统一致的处理能力并完全兼容，配备与主系统相同等级的通信线路和网络设备，对数据远程实时备份，实现数据零丢失。

具体采用何种容灾备份方式，视信息系统重要性、业务特点、建设成本等因素而定。

62 如何制定网络安全事件应急预案？

第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）法律、行政法规规定的其他义务。

关键信息基础设施运营者应当根据《国家网络安全事件应急预案》，制定本部门、本行业、本单位的网络安全事件应急预案。

各部门、行业、单位的网络安全事件应急预案应在网络安全事件分级分类、预警分级等方面与《国家网络安全事件应急预案》保持一致，并在事件处置流程上与《国家网络安全事件应急预案》等上级预案保持衔接。此外，预案中还应明确组织机构与职责，确立本部门、本行业、本单位范围内的预警监测、预警研判和发布、预警响应、预警解除等流程，对事件报告、应急响应、应急结束等程序作出规定，对调查、评估等事项作出安排，并对预案演练、宣传、培训等工作进行规划，此外还应落实技术支撑队伍、专家队伍、社会资源、经费等保障措施。必要时，还应考虑跨部门、跨行业合作及国际合作等问题。

各部门、行业、单位的网络安全事件应急预案与《国家网络安全事件应急预案》的重要区别是，后者是原则性的，但各部门、行业、单位的网络安全事件应急预案应尽可能具体，如应明确到具体的热线联系方式、操作流程细化到每一个动作等。此外，在符合《国家网络安全事件应急预案》中网络安全事件分级分类标准的前提下，各部门、行业、单位可以对每一级的事件进一步细分，并针对每一个细分级别的事件制定不同的处置措施。

63 什么是网络安全审查？

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

网络安全审查是指坚持企业承诺与社会监督相结合，第三方评价与政府持续监管相结合，实验室检测、现场检查、在线监测、背景调查相结合，对网络产品

和服务及其供应链进行网络安全审查。其目的是提高网络产品和服务安全可控水平，防范网络安全风险，维护国家安全。

安全审查的重点是审查网络产品和服务的安全性、可控性，主要包括产品和服务自身的安全风险，以及被非法控制、干扰和中断运行的风险；产品及关键部件生产、测试、交付、技术支持过程中的供应链安全风险；产品和服务提供者利用提供产品和服务的便利条件非法收集、存储、处理、使用用户相关信息的风险；产品和服务提供者利用用户对产品和服务的依赖，损害网络安全和用户利益的风险；其他可能危害国家安全的风险。

国家网信部门已制定印发了《网络产品和服务安全审查办法》，对网络安全审查流程、机构等作出了明确规定。

64 如何判定网络产品和服务可能影响国家安全？

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

产品和服务是否影响国家安全由关键信息基础设施保护工作部门确定。

根据《网络安全法》规定，不是所有的产品和服务都需要审查，而是需要重点关注使用在关键信息基础设施中，可能影响国家安全的产品及服务。应从网络产品的安全性和功能性两个方面判定是否影响国家安全，主要是看产品和服务是否会危害国家政权和主权安全，是否会危害广大人民群众利益，是否会影响国家经济可持续发展及国家其他重大利益。

65 网络安全审查是否要限制国外产品和服务?

网络安全审查不针对特定国家和地区，没有国别差异。这种审查不会歧视国外技术和产品，不会限制国外产品进入中国市场。相反，将会提高消费者对使用产品的信心，扩大企业的市场空间。

国家已经对若干产品和服务进行了网络安全审查，这些产品和服务既有国内的，也有国外的。是否通过审查与国别无必然关系。从实际情况看，并不是国内产品都通过了审查、国外产品都未通过审查。

66 如何理解“使用未经安全审查或者安全审查未通过的网络产品或者服务的”要受到处罚?

第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

《网络安全法》第六十五条中的“使用未经安全审查”的产品或者服务，不是意味着所有的产品和服务都要经过审查，而是指涉及国家安全的产品和服务。

67 关键信息基础设施的运营者采购网络产品和服务时如何签订安全保密协议?

第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

首先，采购的产品和服务可能直接影响国家安全，影响关键信息基础设施的正常运转，影响个人信息和重要数据安全时，应当签订安全保密协议。

其次，安全保密协议应当明确双方的责任义务，包括供应方不非法获取数据、控制关键信息基础设施运转，不无正当理由停止技术支持，未经许可不得泄露、转让关键信息基础设施的敏感数据等。

目前，全国信息安全标准化技术委员会正在组织制定关键信息基础设施安全相关标准，包括安全保密协议模板等。

68 《网络安全法》提出数据应当留存在境内，会不会限制数据跨境流动，影响公民出国旅游和企业跨国贸易？

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

《网络安全法》要求关键信息基础设施运营者在中国境内运营中收集和产生的个人信息及重要数据应当在中国境内存储，确需出境的，应当按规定进行评估，目的是为了维护国家网络安全、保护公民个人利益。

落实法律的要求，要把握以下几点：

一是法律没有要求所有数据的都留在境内，只是对个人信息和重要数据提出要求，而且为确需出境的数据留下了“出口”；

二是对于个人信息而言，经个人明示同意后可以出境，但是，个人主动订购国际机票、拨打海外电话、向境外发送电子邮件等情况，视为已经获得个人同意；

三是法律中的重要数据是对国家而言属于重要的，而不是针对企业和个人。

69 如何理解“境内运营”和“向境外提供”？

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

“境内运营”指网络运营者在中华人民共和国境内开展业务，提供产品或服务的活动。未在境内注册的网络运营者，但在境内开展业务，或向境内提供产品或服务的，也属于“境内运营”。但境内的网络运营者仅向境外机构、组织或个人开展业务或提供产品、服务，且不涉及境内公民个人信息和重要数据的，不属于第三十七条的“境内运营”。

“向境外提供”指网络运营者将其在境内运营中收集和产生的个人信息和重要数据，提供给境外的机构、组织或个人的活动。向本国境内，但不属于本国司法管辖或未在境内注册的主体提供个人信息和重要数据，属于“向境外提供”。数据未转移至本国以外的地方，但被境外机构、组织或个人访问的（公开信息、网页访问除外），属于“向境外提供”。

70 什么是需要在境内存储的“重要数据”？

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境

外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

重要数据是指政府、企业、个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展及公共利益密切相关的数据（包括原始数据和衍生数据），一旦未经授权披露、丢失、滥用、篡改、销毁，或汇聚、整合、分析后，可能造成以下后果：

（一）危害国家安全、国防利益，破坏国际关系；

（二）损害国家财产、社会公共利益和个人合法利益；

（三）影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；

（四）影响行政机关依法调查处理违法、渎职或涉嫌违法、渎职行为；

（五）干扰政府部门依法开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；

（六）危害国家关键基础设施、关键信息基础设施、政府系统信息系统安全；

（七）影响或危害国家经济秩序和金融安全；

（八）可分析出国家秘密或敏感信息；

（九）影响或危害国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施等其他国家安全事项。

全国信息安全标准化技术委员会组织起草了《信息安全技术 数据出境安全评估指南》，其中给出了“重要数据识别指南”。该标准目前正在公开征求意见。

71 数据出境安全评估如何实施？

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境

外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

国家网信部门会同有关部门起草了《个人信息和重要数据出境安全评估办法》，对数据出境安全评估制度作了明确规定。该办法目前正在征求意见。

国家标准《信息安全技术 数据出境安全评估指南》（征求意见稿）给出了数据出境安全评估流程、评估要点和评估方法。

72 跨国公司位于中国和国外的分支机构间传输数据也需要进行安全评估吗?

跨国公司位于中国和国外的分支机构间传输数据也属于跨境传输，如涉及个人信息和重要数据，也需要按照《个人信息和重要数据出境安全评估办法》执行。

从国际上看，由于一些跨国公司的自身结构十分复杂，且分支遍布世界各地，某些国家和地区也专门针对这些问题给出了管理方案。例如，欧盟推出了“有关国际数据转移的约束性企业规则”。约束性企业规则是指由跨国公司集团制定约束企业内部机构间跨境数据流动及个人信息保护的一套行为准则。从功能上说，约束性企业规则是经欧盟认可的向不具备适当数据保护水平的第三国转移数据的依据之一，其仅对集团内公司和员工有约束力。但约束性企业规则仍需经过欧盟数据管理机构的批准。

73 如何理解第六十六条中对在境外存储“网络数据”或者向境外提供“网络数据”的行为的处罚?

第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，

给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

《网络安全法》第六十六条中的“网络数据”指第三十七条中的个人信息和重要数据。

74 如何理解《网络安全法》对关键信息基础设施提出的自评估要求？

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

一是对评估频率提出要求，关键信息基础设施的运营者每年至少进行一次检测评估；二是对评估形式提出要求，运营者应当自行或者委托网络安全服务机构进行评估；三是对评估内容提出要求，对网络的安全性和可能存在的风险进行检测评估；四是对评估结果提出要求，运营者将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

自评估有别于国家网络安全主管部门对关键信息基础设施组织开展的网络安全抽查检测。

自评估不限于任何特定的形式。

75 由谁对关键信息基础设施进行抽查检测和应急演练？

第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

关键信息基础设施保护工作部门应该履行指导、督促关键信息基础设施运行安全保护的职责，组织对本行业、本领域的关键信息基础设施开展抽查检测，以及组织开展本行业、本领域的网络安全应急演练。

国务院电信主管部门、公安部门和其他有关部门，在各自职责范围内可以对关键信息基础设施进行抽查检测。国家网信部门将出台关键信息基础设施抽查检测规范和指南，指导有关部门开展抽查检测，统筹抽查检测计划，避免重复上门，给运营单位带来不必要的负担，并汇总共享抽查检测结果。

76 如何促进网络安全信息共享？

第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

国家网信部门将会同有关部门建立网络安全信息共享机制，制定网络安全信息共享相关技术标准，合法、合理共享网络安全风险、威胁等信息。

第五部分

PART 5

个人信息保护与互联网信息内容安全

77 《网络安全法》为什么加强对个人信息的保护?

第四十条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

中国有 7 亿网民，社会经济高度依赖网络，网络安全不仅关系国家安全、经济发展，也越来越多地关系到广大人民群众的切身利益。目前，我国电信诈骗、信息泄露事件层出不穷，个人信息的泄露、收集、转卖已形成了完整的黑色产业链，公民个人信息安全面临严峻挑战。

《网络安全法》贯彻习近平总书记提出的以人民为中心，网络安全为人民、网络安全靠人民的发展思想，充分借鉴国际惯例，提出了加强个人信息保护的若干规定，以维护广大人民群众在网络空间的安全和利益。作为上位法，这也为今后制定相关管理条例、实施细则和标准规范提供了法律依据。

78 《网络安全法》体现了哪些个人信息保护原则?

《网络安全法》充分借鉴国际上保护个人信息的成熟经验，体现了个人信息安全保护的 8 项重要原则，这些原则也是国际社会公认的个人信息保护基本原则。

（1）责任原则。例如，网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

（2）目的明确原则。例如，网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则。

（3）最少够用原则。例如，网络运营者不得收集与其提供的服务无关的个人信息。

（4）同意和选择原则。例如，收集、使用信息的目的、方式和范围应经被收集者同意。

（5）确保安全原则。例如，网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全。

（6）质量保证原则。例如，用户发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。

（7）主体参与原则。例如，个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息。

（8）开放透明原则。例如，网络运营者应明示收集、使用信息的目的、方式和范围。

79 如何理解《网络安全法》的“明示”要求？

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

《网络安全法》第二十二条、第四十一条均作出了“明示”规定。这里的“明示”应符合以下要求：

一是所明示的内容应易于用户访问，并应确保明示信息的完整性和准确性，如在网站的专门页面、移动应用程序安装页、社交媒体页面等显著位置发布隐私声明或政策；

二是应使所有用户知悉，当逐一告知成本过高或有显著困难时，应能提供合理理由，并以公告的形式告知；

三是内容应清楚、明白、易懂，符合通用的语言习惯，避免使用有歧义的语言；

四是应使用标准化语言、数字、图示等。

对于直接从当事人处获得的个人信息的，应在收集个人信息前予以明示告知。对于非直接从当事人处获得的个人信息的，应在处理个人信息前或在获得个人信息后的合理期限内予以明示告知。

80 如何理解《网络安全法》的“同意”要求？

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

《网络安全法》第二十二条、第四十一条均作出了“同意”规定。这里的同意是指明示同意，即个人信息主体通过书面声明或特定的动作，明确授权对其个人信息进行处理。特别是，收集个人身份证号、银行卡号等敏感信息时，应确保当事人的同意是在其完全知情的基础上自愿给出的、具体的、清晰明确的愿望表示，如个人信息主体主动声明（电子或纸质形式）或主动单击“同意”选项，不得以默许同意方式获取用户同意。

81 如何理解收集个人信息的“合法、正当、必要”原则？

第四十一条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

合法、正当是指，遵循法律法规和公序良俗；履行合同义务所必需；不侵害当事人的利益；维护公共利益所必需。

必要是指，收集的个人信息是提供服务所必需。即网络运营者收集个人信息前，应确定所需收集的个人信息的最小元素集。实际收集的个人信息范围超出个人信息最小元素集时，不得因个人信息主体不同意而拒绝向其提供服务，并仍应保障相应的服务质量。

82 发生或可能发生个人信息安全事件时，应如何告知用户并向主管部门报告？

第四十二条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

全国信息安全标准化技术委员会正在组织制定《个人信息安全规范》，将对如何告知用户并向主管部门报告提出具体要求。此外，国家网信部门正在研究制定的有关数据安全政策中，也会对相关事项提出更高层面的要求，如具体时限、内容、流程等。

一般而言，发生或可能发生个人信息安全事件时，告知内容应包括但不限于：安全事件的内容和影响；已采取或将要采取的处置措施；对当事人自主防范和降低风险的建议；针对当事人提供的补救措施；本单位个人信息安全部门或负责人

的联系方式。应及时将以上信息以邮件、信函、电话、推送通知等方式告知受影响的当事人，难以逐一告知当事人时，应采取合理、有效的方式发布公告。必要时，还应向社会公开披露安全事件相关情况。

83 《网络安全法》规定，个人有权要求网络运营者删除个人信息和纠正不准确的个人信息，这是否会加重企业负担、妨碍企业发展？

第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

《网络安全法》规定，个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息。这包括，即使网络运营者没有违反法律、行政法规的规定，但超出与当事人约定的个人信息保存时限的，也应当删除个人信息，不得在未进行匿名化处理的前提下继续保存和使用。这就是俗称的“被遗忘权”。

采取更加严格的措施保护个人信息安全、维护个人利益，已经成为各国共识。《网络安全法》中关于删除和纠正个人信息的规定，在欧盟《通用数据保护条例》、美国《消费者隐私权利法案》等文件中都有类似表述。

企业和机构应该把保护个人信息安全和信息的准确性作为应尽义务，而不应视为额外负担。与此同时，在法律的实施过程中，要科学平衡保障安全和促进企业创新的关系，既充分保障个人信息安全，又不妨碍企业创新和发展。

84 个人如何“发现”网络运营者违法或违反约定收集、使用个人信息或收集、存储的个人信息有错误？

第四十三条 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

《网络安全法》第四十三条的要求对保护用户个人信息安全十分重要。例如，银行系统中存储了用户的大量信息，这些信息的准确性直接关系用户利益，用户的联系方式等都应保持有效、可用，因此必须确保用户对这些个人信息有知情权。但是，网络运营者是否违法或违反约定收集、使用个人信息，或者收集、存储的个人信息是否需要更正，这不能依靠用户“偶然发现”。为了落实该条的要求，网络运营者应当允许当事人可以获取其所提供的个人信息的副本，或依其要求在技术可行的前提下直接将副本传输给第三方。

在验证当事人身份后，网络运营者应及时响应当事人提出的请求。

85 如何理解不得非法出售或者非法向他人提供个人信息？

第四十四条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

近年查获曝光的大量案件显示，公民个人信息的泄露、收集、转卖，已经形成了完整的黑色产业链。个人信息的泄露和非法信息买卖又进一步助长了精准诈骗、社会工程学入侵网络等恶意违法行为。

为此，《网络安全法》第四十四条规定，不得非法出售或者非法向他人提供个人信息。根据此条的精神，个人信息原则上不得转让、披露，更不允许出售。确需转让、披露甚至出售时，应满足合法性要求，具体包括：

（1）事先征得当事人明示同意；

（2）事先开展安全风险评估，并依评估结果采取有效安全措施；

（3）承担因转让、披露个人信息对当事人造成损害的相应责任；

（4）不得违反相关法律法规。

转让方有义务帮助当事人了解受让方对个人信息的存储、使用等情况。当事人请求删除其个人信息时，转让方应同时通知受让方及时删除。特别是，当受让方发生个人信息安全事件，对当事人造成损害时，转让方有责任帮助当事人追究受让方责任。

86 《网络安全法》规定，网络运营者应当加强对其用户发布的信息的管理，这是否会妨碍网上言论自由和信息自由流动？

第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

中国坚持积极利用、科学发展、依法管理、确保安全的方针，在推进互联网发展、加强互联网管理过程中，充分保障人权和言论自由，充分尊重广大人民群

众的知情权、参与权、表达权和监督权。同时，也强调任何人、任何机构都应该对自己在网上的言行负责，个体的自由不应以损害他人的自由和社会公共利益为代价，任何人和机构都有义务自觉维护网络秩序，自觉维护网络安全。

对这条规定有两点理解：第一，针对的是用户公开发布的信息，而不是个人通信信息，不会侵害用户通信自由和通信秘密；第二，要求停止传输的是违法信息，不存在妨碍言论自由问题。

87 网络运营者删除用户发布的信息，应当遵循哪些要求？

根据《网络安全法》第四十七条、第五十条要求，网络运营者发现法律、行政法规禁止发布或者传输的信息的，或国家网信部门和有关部门发现此类信息后通知网络运营者的，网络运营者应当依法立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录。

根据《网络安全法》第四十九条要求，网络运营者删除用户发布的信息，应当符合法律法规的要求，遵循与用户的合同约定，充分保护用户依法使用网络的权利。对已删除的用户信息，应当建立投诉制度，及时响应当事人或当事机构的投诉。

88 《网络安全法》中的“电子信息发送服务提供者”、“应用软件下载服务提供者”有哪些？

第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安

全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

电子信息发送服务提供者包括即时通讯服务提供者、电子邮件服务提供者、信息发布服务提供者等。

应用软件下载服务提供者主要指各类应用软件商店、提供软件下载服务的网站等。

89 如何理解电子信息发送服务提供者和应用软件下载服务提供者的安全管理义务？

第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

《网络安全法》第四十八条规定了电子信息发送服务和应用软件下载服务提供者的安全管理义务。理解此条时，需要把握电子信息发送和应用软件下载的重大区别。前者可能涉及点对点的个人通信，公民的通信自由和通信秘密受《宪法》保护。因此，电子信息发送服务提供者在“知道”其用户在发送的电子信息中设置了恶意程序，或含有法律、行政法规禁止发布或者传输的信息，才可采取处置措施。但这不意味着电子信息发送服务提供者可以监测用户的点对点通信内容。但是，当信息的接收者达到一定规模，已经不属于个人通信时，电子信息发送服务提供者还是应当履行对信息的监测义务。

90 《网络安全法》要求采取技术措施和其他必要措施阻断境外非法信息的传播，这是否意味着要对国外网站进行更严格的封堵？

第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

现实世界中，无论是企业还是个人，进入哪个国家就要遵从哪个国家的法律法规要求，任何非法行为都会受到法律的制裁。当前，网络已经成为经济发展、生产生活的重要平台，网络空间不是法外之地。在中国境内的网络，包括网络上的信息及与网络相关的行为，都必须遵守中国的法律。《网络安全法》要求阻断的是非法信息的传播，目的是保障网络信息依法、自由、有序流动。

第六部分

PART 6

监测预警与应急处置

91 为什么要建立网络安全监测预警和信息通报制度，并加强统筹协调？

第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

网络安全监测预警和信息通报工作可以使网络运营单位及时采取措施防范风险、消除隐患、应对威胁、处置事件，尽可能预防和减小网络安全事件造成的损失和危害。建立网络安全监测预警和信息通报制度有利于明确相关部门的职责，规范预警和信息通报行为，促进网络安全信息的共享和利用。

目前，我国已有多个部门建立了网络安全监测预警和信息通报制度。这些制度之间缺少协同，标准不统一，存在各自发布预警通报、应急预案体系不完整、不协调等问题。此外，一些企业也在自行发布网络安全监测预警信息。《网络安全法》要求，国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照《国家网络安全事件应急预案》的规定，统一发布网络安全监测预警信息。

92 各行业、各领域的网络安全监测预警信息如何报送？

第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

根据《网络安全法》，负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。负责关键信息基础设施保护工作的部门，除按原有渠道报送网络安全预警信息外，还应向国家网信部门报送。

《国家网络安全事件应急预案》对各地区、各部门报告网络安全事件相关信息作了规定，要求各省（区、市）、各部门将重要监测信息报国家网络安全应急办公室（设在国家网信部门），对可能发生重大及以上网络安全事件的信息、本地区本行业的橙色预警应及时报告应急办公室，初判为特别重大、重大网络安全事件的信息应立即报告应急办公室。

93 各行业、各领域网络安全应急预案与国家网络安全应急预案的关系是什么?

第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

各部门应该根据《国家网络安全事件应急预案》制定或修订本行业、本领域的网络安全事件应急预案，并做好与国家预案的衔接。衔接主要体现在各行业、各领域网络安全事件预案在事件分级、应急指挥、预警发布、信息报告等方面应该与国家预案中的相关规定保持一致或与相关机制相衔接。

94 网络安全事件如何分级？

第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

《国家网络安全事件应急预案》根据事件对重要网络和信息系统造成的损失程度，对国家安全、社会秩序、经济建设、公众利益等构成的威胁和造成的影响程度，将网络安全事件分为特别重大、重大、较大、一般事件等四级。

国家标准 GB/Z 20986-2007《信息安全技术 信息安全事件分类分级指南》对网络安全事件的分类和分级给出了具体说明。

95 如何理解网络安全事件处置的属地管理规定？

第五十四条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

（二）组织有关部门、机构和专业人员，对网络安全风险信息进行

分析评估，预测事件发生的可能性、影响范围和危害程度；

（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

《网络安全法》授权省级以上人民政府有关部门，在网络安全事件发生的风险增大时，采取有关措施。这一规定充分考虑了很多重要关键信息基础设施垂直管理的实际情况。对垂直管理的关键信息基础设施，虽然其网络安全保护工作部门不是地方政府，但其一旦出现网络安全事件，将对地方公共安全、经济发展、群众利益产生直接影响。在这种情况下，有必要明确地方政府部门在处置网络安全事件、风险时的权限。这既是一种授权，也是一责任。

根据《网络安全法》，《国家网络安全事件应急预案》进一步规定，各省（区、市）网信部门在本地区党委网络安全和信息化领导小组统一领导下，统筹协调组织本地区网络和信息系统网络安全事件的预防、监测、报告和应急处置工作。

96 发现安全风险或发生安全事件时，如何对该网络运营者进行约谈？

第五十六条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

网信、电信、公安等部门，可以根据网络安全风险或网络安全事件的影响和危害情况，在职责范围内视情约谈网络运营者，主要是提醒督促网络运营者采取措施防范风险、消除事件产生的危害。相关行业的主管监管部门也可以按照法律的规定约谈本行业、本领域的网络运营者。

97 什么情况下需要采取通信管制临时措施?

第五十八条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

通信管制属于一种在特定区域、特殊情况下实施的临时措施。只有当国家安全和社会公共秩序受到威胁，或者出现严重恐怖和重大突发社会安全事件时，才可实施通信管制，如阻断恐怖分子通过网络进行的策划、勾连等活动。当今时代，经济社会运行已经全面依赖互联网等通信网络，通信管制可能会对生产生活造成重大影响。《网络安全法》规定，通信管制必须经过国务院决定或者批准后方可实施。地方政府和任何其他部门没有这样的权限。而且通信管制的实施范围、持续时间应受到严格限制，并对可能造成的影响制定好预案。

第七部分

PART 7 其　他

98 如何区分“网络运营者”中“网络的所有者、管理者和网络服务提供者”？

第七十六条 本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

《网络安全法》第七十六条定义，“网络运营者”包括“网络的所有者、管理者和网络服务提供者”。实际工作中，这三类角色往往不是由同一主体承担的。“所有者”强调属主概念，即网络资产的实际所有人。“管理者”不能理解为网络的主管部门，而是实际负责网络运行的组织。这类似于某个大厦，其产权所有人和物业公司不是同一家，但大厦出现事故，产权所有人和物业公司各自承担相应的不同责任。

“网络服务提供者”包含的主体很多。从电信行业管理角度看，既包含接入服务提供者（ISP），也包含网络内容服务提供者（ICP）。前者可以是网络的所有者或管理者，后者则一般有别于网络的所有者和管理者。但广义上，只要通过

网络和信息系统对外提供特定的功能，都可以认为是网络服务提供者。

99 违反《网络安全法》的行为如何记入信用档案？

第七十一条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

《网络安全法》第七十一条的目的是进一步加大对违反《网络安全法》行为的惩戒力度。

根据 2013 年 3 月 15 日起施行的《征信业管理条例》，中国人民银行及其派出机构依法对征信业进行监督管理。该条例进一步明确，设立经营个人征信业务的征信机构，应当符合《中华人民共和国公司法》规定的公司设立条件和《征信业管理条例》设定的条件，并经国务院征信业监督管理部门批准。除社会机构根据上述规定依法设立的征信机构外，国家还设立了金融信用信息基础数据库，由中国人民银行监督管理。

此外，一些组织包括政府机构在开展工作的过程中，也建立了本组织范围内的“诚信档案”，如招考机构对考生建立的“诚信档案”，这是一种内部的管理行为。

《网络安全法》中的信用档案是个统称的概念，未限定违法行为记入哪一类信用档案。鼓励各类征信机构或建有信用档案的机构将是否违反网络安全法作为评价企业或个人信用的重要参考。

100 如何对来源于境外的机构、组织、个人危害国家关键信息基础设施的活动追究其责任？

第七十五条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

国家关键信息基础设施是网络安全的重中之重，境外机构、组织、个人危害我国关键信息基础设施，即已触犯我国法律，必须受到法律制裁。一方面，国家积极开展双边、多边国际合作，共同打击跨国网络违法犯罪；另一方面，境外机构、组织、个人从事危害我国关键信息基础设施的行为并造成严重后果的，其一旦进入我国司法管辖范围开展活动，国家将行使司法管辖权，追究违法主体责任。即使行为人本身不在我国境内，但其财产处于我国司法管辖权范围内，国务院公安部门和有关部门也可决定对其采取冻结财产或者其他必要的制裁措施。这是依法行使网络空间国家主权的必然要求。

附录 A

APPENDIX A

中华人民共和国网络安全法

目　录

第一章　总则

第一条　为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条　在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条　国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第四条　国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第五条　国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第六条　国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第七条　国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第八条　国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第九条　网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会

的监督，承担社会责任。

第十条 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第十一条 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第十二条 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十三条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第十四条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章 网络安全支持与促进

第十五条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理

以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第十六条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

第十七条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第十八条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

国家支持创新网络安全管理方式，运用网络新技术，提升网络安全保护水平。

第十九条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第二十条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第三章 网络运行安全

第一节 一般规定

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第二十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十三条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十四条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二十五条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十六条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第二十八条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第二十九条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节 关键信息基础设施的运行安全

第三十一条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第三十二条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十四条 除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）法律、行政法规规定的其他义务。

第三十五条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十六条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十七条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第三十九条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第四章　网络信息安全

第四十条　网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

第四十一条　网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十二条　网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十三条　个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十四条　任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十五条　依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十六条　任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管

制物品以及其他违法犯罪活动的信息。

第四十七条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第四十八条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第四十九条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第五章 监测预警与应急处置

第五十一条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十二条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第五十三条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络

安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第五十四条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第五十五条 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第五十六条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第五十七条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第五十八条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第六章 法律责任

第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网

络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

第六十条 违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

第六十一条 网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十二条 违反本法第二十六条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告；拒不改正或者情节严重的，处一万元以上十万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五千元以上五万元以下罚款。

第六十三条 违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全

的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

违反本法第四十四条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款。

第六十五条 关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十六条 关键信息基础设施的运营者违反本法第三十七条规定，在境外存储网络数据，或者向境外提供网络数据的，由有关主管部门责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十七条 违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、

通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，

可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第六十八条 网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处十万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。

第六十九条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

（一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的；

（二）拒绝、阻碍有关部门依法实施的监督检查的；

（三）拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十条 发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的，依照有关法律、行政法规的规定处罚。

第七十一条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第七十二条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接

责任人员依法给予处分。

第七十三条 网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第七十四条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七十五条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章 附则

第七十六条 本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、

身份证件号码、个人生物识别信息、住址、电话号码等。

第七十七条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第七十八条 军事网络的安全保护，由中央军事委员会另行规定。

第七十九条 本法自 2017 年 6 月 1 日起施行。

附录 B

APPENDIX B

网络产品和服务安全审查办法（试行）

第一条 为提高网络产品和服务安全可控水平，防范网络安全风险，维护国家安全，依据《中华人民共和国国家安全法》《中华人民共和国网络安全法》等法律法规，制定本办法。

第二条 关系国家安全的网络和信息系统采购的重要网络产品和服务，应当经过网络安全审查。

第三条 坚持企业承诺与社会监督相结合，第三方评价与政府持续监管相结合，实验室检测、现场检查、在线监测、背景调查相结合，对网络产品和服务及其供应链进行网络安全审查。

第四条 网络安全审查重点审查网络产品和服务的安全性、可控性，主要包括：

（一）产品和服务自身的安全风险，以及被非法控制、干扰和中断运行的风险；

（二）产品及关键部件生产、测试、交付、技术支持过程中的供应链安全风险；

（三）产品和服务提供者利用提供产品和服务的便利条件非法收集、存储、处理、使用用户相关信息的风险；

（四）产品和服务提供者利用用户对产品和服务的依赖，损害网络安全和用户利益的风险；

（五）其他可能危害国家安全的风险。

第五条 国家互联网信息办公室会同有关部门成立网络安全审查委员会，负责审议网络安全审查的重要政策，统一组织网络安全审查工作，协调网络安全审查相关重要问题。

网络安全审查办公室具体组织实施网络安全审查。

第六条 网络安全审查委员会聘请相关专家组成网络安全审查专家委员会，在第三方评价基础上，对网络产品和服务的安全风险及其提供者的安全可信状况进行综合评估。

第七条 国家依法认定网络安全审查第三方机构，承担网络安全审查中的第三方评价工作。

第八条 网络安全审查办公室按照国家有关要求、根据全国性行业协会建议和用户反映等，按程序确定审查对象，组织第三方机构、专家委员会对网络产品和服务进行网络安全审查，并发布或在一定范围内通报审查结果。

第九条 金融、电信、能源、交通等重点行业和领域主管部门，根据国家网络安全审查工作要求，组织开展本行业、本领域网络产品和服务安全审查工作。

第十条 公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过网络安全审查。产品和服务是否影响国家安全由关键信息基础设施保护工作部门确定。

第十一条 承担网络安全审查的第三方机构，应当坚持客观、公正、公平的原则，按照国家有关规定，参照有关标准，重点从产品和服务及其供应链的安全性、可控性，安全机制和技术的透明性等方面进行评价，并对评价结果负责。

第十二条 网络产品和服务提供者应当对网络安全审查工作予以配合，并对提供材料的真实性负责。

第三方机构等相关单位和人员对审查工作中获悉的信息等承担安全保密义务，不得用于网络安全审查以外的目的。

第十三条 网络安全审查办公室不定期发布网络产品和服务安全评估报告。

第十四条 网络产品和服务提供者认为第三方机构等相关单位和人员有失客观公正，或未能对审查工作中获悉的信息承担安全保密义务的，可以向网络安全审查办公室或者有关部门举报。

第十五条 违反本办法规定的，依照有关法律法规予以处理。

第十六条 本办法自 2017 年 6 月 1 日起实施。

附录 C

APPENDIX C

重要数据识别指南（征求意见稿）

指南中的重要数据是指我国政府、企业、个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据（包括原始数据和衍生数据），一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能造成以下后果：

（一）危害国家安全、国防利益，破坏国际关系；

（二）损害国家财产、社会公共利益和个人合法利益；

（三）影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；

（四）影响行政机关依法调查处理违法、渎职或涉嫌违法、渎职行为；

（五）干扰政府部门依法开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；

（六）危害国家关键基础设施、关键信息基础设施、政府系统信息系统安全；

（七）影响或危害国家经济秩序和金融安全；

（八）可分析出国家秘密或敏感信息；

（九）影响或危害国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施等其他国家安全事项。

根据上述定义和行业（领域）主管部门相关规定，指南提出了各行业（领域）重要数据的范围。请各行业（领域）主管部门结合实际，明确本行业（领域）重要数据定义、范围或判定依据；并根据行业（领域）发展变化，及时更新或替换本指南中相关内容。

本指南不影响中国在《世贸组织协定》等国际协定项下义务的执行。

1 石油天然气

主管部门：国家发展改革委、能源局。

重要数据包括但不限于：

a）价值类，包括表示资源金额等信息；

b）生产量类，包括各类生产量等信息；

c）销售量类，包括各类销售量等信息；

d）施工作业量类，包括各类施工作业量等信息；

e）安全与环保类，包括计量管理、节能管理、劳保用品、危险作业区、质量控制等信息；

f）储备类，包括储备数量、储备设施位置、坐标等信息。

2 煤炭

主管部门：国家发展改革委、能源局。

重要数据包括但不限于：

a）行业基本情况，主要包括企业数量、企业分布、企业类型、从业人员数量、从业人员分布等；

b）行业经济情况，主要包括行业的资产、负债、收入、利润、主要经济指标、行业资金紧张程度等；

c）行业采购情况，主要包括原材料的采购量、采购金额、采购价格以及采购周期等；

d）行业生产情况，主要包括行业的产值、生产投入、劳动生产率、产能以及产能影响因素等；

e）行业销售情况，主要包括行业市场规模、销售投入、人均销售水平、主要产品销售价格等；

f）行业投资情况，主要包括行业新建项目数量、投资额、资金来源等。

3 石化

主管部门：能源局。

重要数据包括但不限于：

a）国家石油、石化工业年度和中、长期发展规划的主要经济技术指标和重大政策措施；

b）石化工业重要生产物资年度进口计划和未分配的控制外汇金额。

4 电力

主管部门：国家发展改革委、能源局。

重要数据包括但不限于：

4.1 发电厂相关信息

a）火电厂的用煤量、水电厂的耗水量等信息；

b）发电机组数据，包括火电、水电等发电机组可靠性指标数据等信息；

c）电厂内变电站的开关数据，包括厂站名、开关类型、电抗值、母线电压、投入时间、退出时间等信息。

4.2 输配电信息

a）实际负荷、预测负荷等信息；

b）输变电设备可靠性指标，包括电压等级、统计百台年数、故障率、故障次数、故障停运时间、修复时间、计检率、计检平均时间等信息；

c）输电线路信息，包括线路段号、侧地名、侧开关号、并联号、侧省名、调度权、线路长度、导线型号、地线型号、安全电流、控制电流、导线排列、正序电阻等；

d）线损消耗、影响线路状态的环境信息等。

4.3 建设运维信息

a）装机容量、发电量、供应量等信息；

b）同比、环比增减量等信息；

c）电力各系统配置信息，包括配电自动化系统、生产管理系统、停电管理系统、高级量测体系、电能质量监控系统、用户能效管理系统等；

d）电力各系统运行信息，包括电压、电流、频率、波形等；

e）电力系统实时状态监控、电力系统巡检、电力调度等信息；

f）可靠性统计分析信息，包括可用系数、强迫停运率、平均无故障可用小时、故障率、修复率等。

4.4 其他信息

a）电力各系统资产、配套安防系统相关信息；
b）未发布的电网 / 电厂规划图等；
c）城市电网管线分布图文资料；
d）电网地理坐标信息；
e）能够有助于入侵攻击电力基础设施的其他信息。

5 通信

主管部门：工业和信息化部。
重要数据包括但不限于：

5.1 规划建设类数据

主要包括电信网和互联网网络及信息系统在规划及建设环节产生的重要数据，如规划设计及建设方案、灾难备份系统设计及建设方案、设备地理位置、网络拓扑结构、线路路由走向、设备资产采购清单等。

5.2 运行维护类数据

主要包括网络及信息系统运维过程中产生、收集的重要数据，如设备及软件配置信息、IP 地址分配信息及内外网转换信息、网络流量流向信息、网络及系统运行状态信息、网络及系统运行维护日志，以及系统用户资料信息等。

5.3 安全保障类数据

a）网络与信息安全管理数据，如网络安全预警监测信息、系统及数据访问操作日志、安全审计记录、网络安全应急预案、违法有害信息监测处置相关数据、

用户访问互联网日志数据、用户计费数据和上网记录等个人通信数据；

b）应急通信数据，如应急通信系统规划、建设、运行相关信息等；应急通信事件分级信息和应急预案，重大活动行动方案、保障预案信息、应急通信装备物资储备、保障队伍部署等。

5.4 无线电数据

a）国家重要行业，如交通运输、渔业、海洋系统、航空、航天、军事、广播电视等行业使用的涉及国家主权、安全的无线电频率和台站信息；

b）卫星通信信息主要是指使用卫星进行通信所涉及的相关信息，主要包括卫星地面站基建、卫星地面站灾备、卫星通信用户等信息；

c）蜂窝移动通信基站位置、蜂窝移动通信基站基建、蜂窝移动通信基站灾备、蜂窝移动通信基站收发能力等信息；

d）无线电监测信息主要指开展无线电监测工作所涉及的相关信息，主要包括无线电监测站地理位置、天线配置、设备能力等监测设施信息，以及监测信号样本、频段扫描数据、频率时间占用度等电磁环境信息；

e）上述信息中已纳入国际电信联盟（ITU）国际频率登记总表（Master International Frequency Register，MIFR）内的信息除外；国家无线电管理机构正在向或需向 ITU 进行申报的无线电网络数据除外。

5.5 统计分析类数据

主要包括：根据网络及信息系统运行、用户网络行为等过程中直接产生、收集的重要数据，以及统计分析得到的数据，如行业和企业运行情况、用户网络行为习惯分析信息、行业或业务发展预测信息等。

5.6 其他通信数据

a）关键基础设施网络威胁源数据；

b）通信内容、信令、记录等数据；

c）基础核心技术、核心设备主要性能参数、网络信息安全整体防护能力。

6 电子信息

主管部门：工业和信息化部。

重要数据包括但不限于：

a）产业运行数据，主要包括：尚未公开的规模以上电子信息产业企业数量、产值、销售收入、利润等基本情况，尚未公开的产业新在建项目数量、项目可行性报告、投资额、资金来源等投资情况，及尚未公开的电子信息产品进出口贸易情况；

b）产业发展数据，主要包括：尚未公开的产业发展规划、发展重点、近期国家级和部重点的研发支持项目等；

c）电子信息百强企业业务数据，主要包括：尚未公开的企业业务发展决策、投融资决策，及企业产值、销售收入、利润、研发投入、研发人员数量等内容；

d）电子信息产品基础硬件的型号、重要参数、源代码和目标、技术方案、实验数据、检测报告、重要工艺技术等全部技术资料；

e）国防军事领域、政务领域和公共服务领域等在关键领域或重要行业中各类电子信息设备的销售信息和使用信息，例如购买方名单、交易价格、交易数量、采购周期、采购产品型号、应用领域、产品去向、更换频率等；

f）在关键领域或重要行业中电子信息产品在使用过程中的运行、保养和维修信息，例如使用信号波段、频率等设备运行参数，设备故障频率、故障原因、解决方案、使用寿命等维修记录；

g）在关键领域或重要行业中电子信息产品在使用过程中采集、存储、管理和分析的涉及政府秘密、商业秘密和个人隐私的信息。包括地理地貌、气候环境、卫星轨道、军事部署等相关信息，企业、单位决定不宜公开的商业资料及个人隐私，包括个人身份信息、财产信息、健康信息等。

7 钢铁

主管部门：工业和信息化部。

重要数据包括但不限于：

7.1 钢铁产业的实力、潜力及竞争力信息

a）重点区域或企业的生产安排、炼钢配比、规模、产量、生产设备与技术水平、采购计划、物流配送、能耗等信息；

b）企业重点产品批量进入石油、化工等重点领域和新兴领域的信息；

c）大型客户采购钢铁的品种、频次、吨数等信息。

7.2 国防军用和国民经济建设发展所需钢材、优特钢产业等实力信息

涉及冶金、能源、交通、建筑、桥梁、机械、电子等国民经济建设发展所需先进钢铁材料及其制品的信息。

7.3 国家产业发展及外部环境掌控、应对相关信息

a）钢铁市场行情的预测和动态监测方面的信息；

b）钢铁行业未公开的政策文件、布局安排、军民配置分配、统计数字等相关信息。

8 有色金属

主管部门：工业和信息化部。

重要数据包括但不限于：

8.1 有色金属产业的实力、潜力及竞争力信息

a）重点企业的生产安排、规模、产量、生产设备与技术水平、采购计划、物流配送、能耗、销售去向、贸易谈判等信息；

b）大型客户采购有色金属的品种、频次、吨数等数据。

8.2 国防军工和国民经济建设发展所需有色金属信息

有色金属产品的名称、科研、勘察开采计划，生产能力、工艺技术路线，全

部技术资料，企业名称、产地、产量、产能、储备、消费去向等信息及统计信息。

8.3 国家有色金属产业发展及外部环境掌控、应对信息

有色金属市场行情的预测和动态监测方面的信息。

9 装备制造

主管部门：工业和信息化部。

重要数据包括但不限于：

9.1 投资信息

生产安全保障类装备和高技术关键装备，如军事、航空航天装备等的投资信息。

9.2 重要装备出厂后工程活动信息

国民经济、国防施工等重要领域装备长时间或大范围生产活动相关信息。

10 化学工业

主管部门：工业和信息化部。

重要数据包括但不限于：

a）国家主要化工产品生产能力、储备情况等统计信息，重大化工进出口项目相关信息；

b）重要地区化工经济项目协议、项目、计划及军用化学品出口相关信息等；

c）剧毒化学品、易爆危险化学品的道路运输、水路运输、航空运输等相关信息；

d）生产、储存危险化学品的单位，其作业场所设置通信、报警装置、警卫保护措施等相关信息；

e）机构出具的对化工企业的安全生产条件进行评价的报告；

f）新建、改建、扩建生产、储存危险化学品的建设项目，以及新建、改建、扩建储存、装卸危险化学品的港口建设项目信息；

g）化工厂房平面图、化学品存储库房分布、库场面积、容量、年度用量、来源等资料；

h）企业生产、储存的剧毒化学品、易致爆危险化学品的数量、流向等相关信息。

11 国防军工

主管部门：国防科工局。

其重要数据包括但不限于：

a）采购元器件、软件、型号材料、工控设备测试仪器的名称、数量、来源、途径、代理商等信息；

b）军工科研生产单位内部名称、地理位置、建设计划、安防规划、保密等级、警卫保护、厂房图纸、库房容积、储备情况等信息。

12 其他工业

主管部门：工业和信息化部。

重要数据包括但不限于：

a）战争及临时宣布的紧急备战时期，全国及各大地区军用产品的运输、储备计划和执行情况；

b）处于世界先进水平，且对国民经济具有重要影响的工业研究开发项目、计划；

c）具有国际水平和重大经济效益的科研成果中的核心部分；

d）全国输油、输气管线及战备油库的坐标；

e）全国石油库存的分布、统计数字及有关资料；

f）涉及国防军工生产的发供用电规划、计划和统计资料；

g）工业科技发展重点任务中与安全相关的关键科技内容。

13 地理信息

主管部门：国土资源部（国家测绘地理信息局、国家海洋局）。

重要数据包括但不限于：

13.1 重要目标地理信息

a）标注国家或地区重要安全警卫目标、设施和关键基础设施信息的遥感影像；

b）国家或地区重要安全警卫目标、设施和带有位置精度信息的实景影像；

c）分辨率和位置精度优于遥感影像公开使用要求的影像；

d）大于 1:5 万（含）比例尺海图及其数字化成果；

e）大于 1:5 万（含）比例尺地形图及其数字化成果；

f）未经审核发布的重要地理信息，包括国界、国家海岸线长度；领土、领海、毗连区、专属经济区面积；国家海岸滩涂面积、岛礁数量和面积；国家版图的重要特征点，地势、地貌分区位置；国务院测绘地理信息行政主管部门商国务院其他军地有关部门确定的其他重要自然和人文地理实体的位置、高程、深度、面积、长度等地理信息；

g）地理信息分析数据，包括能源、金属、非金属等主要矿物的地理分布情况及开采储量、设计储量、远景储量等储量信息，尤其是与国家安全密切相关的矿产情况。

13.2 标识有下列内容的（对社会公众开放的除外）地理信息

a）专用铁路及站内火车线路、铁路编组站，专用公路；

b）未经国家有关部门批准公开发布的与地理相关的重大经济建设信息等；

c）未公开的机场（含民用、军民合用机场）和机关、单位的信息；

d）国家法律法规、部门规章禁止公开的其他内容。

13.3 标识有下列目标具体形状及属性的（用于公共服务的设施可以标注名称）地理信息

a）大型水利设施、电力设施、通信设施、石油和燃气设施、重要战略物资储备库、气象台站、降雨雷达站和水文观测站（网）等涉及国家经济命脉，对人民生产、生活有重大影响的民用设施；

b）监狱、看守所、拘留所、强制隔离戒毒所等与公共安全相关的单位；

c）公开机场的内部结构及运输能力属性；

d）渡口的内部结构及属性；

e）国家法律法规、部门规章禁止公开的其他内容相关形状和属性。

13.4 标识有下列内容属性的地理信息

a）高压电线、通信线、管道的属性；

b）国家法律法规、部门规章禁止公开的其他内容相关属性；

c）水库库容、输电线路电压等精确数据，桥梁、渡口、隧道的结构形式和河底性质，未经公开的港湾、港口、沿海潮浸地带的详细数据；

d）重要桥梁的限高、限宽、净空、载重量和坡度属性，重要隧道的高度和宽度属性，公路的路面铺设材料属性；

e）江河的通航能力、水深、流速、底质属性，水库的库容属性，拦水坝的构筑材料和高度属性，水源的性质属性，沼泽的水深和泥深属性。

13.5 特殊测绘信息

a）国家重力控制点成果、加密重力测量成果，航空重力测量成果、海洋重力测量成果，以及小于5×5分辨率的平均重力异常和似大地水准面成果等各类计算衍生产品；

b）军事禁区的磁力测量数据和我国海域磁力测量数据及其衍生品；

c）境内优于25米网络的数字高程模型、数字地表模型数据。

13.6 公开地图数据

按照2015年12月颁布的《地图管理条例》（国务院第664号令），互联网地图服务单位应当将存放地图数据的服务器设在中华人民共和国境内，并将互联网服务单位收集、使用、提供的用户位置相关信息存放在中华人民共和国境内。

13.7 北斗卫星导航信息

a）北斗卫星导航系统的灾备和服务能力等数据；

b）北斗卫星导航系统生成和服务的高精度位置数据；

c）北斗卫星导航用户名录、属性、装备识别号（ID）及短信息服务内容等数据。

14 民用核设施

主管部门：国防科工局和能源局。

安全监管部门：环境保护部（国家核安全局）。

重要数据包括但不限于：

14.1 民用核设施安全监管信息

a）管理部门对于建造、装料、运行、退役等活动审批中涉及的关键设计资料、运行参数等；

b）未公布的全国辐射环境监测原始信息。

14.2 民用核设施运行信息

a）核燃料生产、加工、贮存和后处理设施、放射性废物处理设施中涉及的关键技术电子资料，如关键设备设计图纸、制造工艺等信息；

b）核动力厂（核电站、核热电厂、核供气供热厂等）的产能，核燃料年度采购处置数量及处置信息，业务信息系统中重要业务统计信息，日常运维管理信息（如重大核电厂运行异常大事件、停堆换料或检修等）；

c）其他反应堆（研究堆、实验堆、临界装置等）的使用信息、核燃料年度采购处置数量及处置信息，业务信息系统中重要业务数据统计信息，日常运维管理的信息（如停堆换料或检修等）；

d）核燃料生产、加工、贮存和后处理设施的年度处理能力、年度处理记录、原料采购、产品销售等相关统计信息、业务系统中的业务信息；

e）放射性废物处理和处置设施的年度处理能力、年度处理记录、原料采购、产品销售等相关统计信息，业务系统中的业务信息；

f）核动力厂、反应堆、核燃料加工处理等机构为满足监管要求建立的通信网络相关信息，以及上报的停堆换料或检修等信息；

g）对核设施工况参数进行监控而使用的核设施数据采集系统形成的信息。

14.3 核设施产业发展信息

a）我国核原料矿产分布、储量等信息；

b）国家发展规划中关于民用核设施的发展规划信息；

c）民用核设施科研中的试验或测试数据。

注：依据我国有关法律法规及参加的国际公约，以上信息中已公开的除外。

15 交通运输

主管部门：国家交通战备办公室、交通运输部、国家铁路局、中国铁路总公司。

重要数据包括但不限于：

15.1 含有下列内容，或通过汇聚分析能印证、推论出下列信息的数据

交通运输相关的信息通信系统部署信息、无线电频谱（有公开标准、依照国家公约、国内法律法规规定的除外）。

15.2 以下各个具体领域的属性数据单点可被测定或公开，但集中批量的数据泄露可能会危害国家安全、军事行动或反恐安全

a）关键铁路线路图、车站布局、轨道分布、仓储数据等资料；

b）涉外交通运输工程施工建设过程中的地理、水文、技术资料、统一口径等数据。

16 邮政快递

主管部门：邮政局。

重要数据包括但不限于：

a）与客户签署保密协议或协议中保密条款约定的不能共享使用的信息；

b）邮政服务过程中的名址、联系电话、数量金额等信息；

c）邮政企业、快递企业的运单数据，如收寄物品的名称、规格、数量、重量、收寄时间、寄件人和收件人名址、联系电话，以及寄递过程中的实时位置、位置轨迹、车辆、人员等信息；

d）邮政企业、快递企业收集的上下游用户相关名址数据，涵盖企业、个人客户的客户名单、客户姓名或单位名称、网址或地址、联系电话等信息；

e）收寄邮件、快件时登记的上下游用户实名身份证件信息；

f）通过大数据分析得到涉及特定个体用户数据，如姓名、住址、身份证号、联系方式等；

g）有助于黑客实施攻击邮政行业的数据，与基础设施、网络、系统等方面相关的材料，包括但不限于系统架构设计说明文档、基础设施的布局和建设文档、网络架构设计文档、IP 地址分配文档、主要软硬件类型、维护人员信息、维护用户账号和密码等。

17 水利

主管部门：水利部。

重要数据包括但不限于：

a）水情信息拍报电码；

b）未经国际防汛抗旱总指挥部批准公布，可能造成重大灾情的水、旱情信

息及预报成果；

c）大型及防洪重点水库运行管理资料；

d）大型水利水电、水利枢纽、跨流域调水等重要工程项目的规划、项目建议书、可行性研究、初步设计、施工、竣工验收报告、图纸等资料及系统水文分析成果；

e）省、流域机构水利发展的中、长期计划；

f）七大江河流域及重要地区水的中、长期供求计划；

g）涉及对外技术合作和水利工程合作项目的未公开出版的科技成果、资料；

h）反映大、中型水库移民生活的资料及水库移民专项资金的年度计划；

i）水文、水质年鉴、水情年报、水情资料汇编和水文公报（含水质通报、水资源公报等）；

j）传输网络中的实时水文与工程运行信息；

k）省际水事纠纷及水事违法案件、水土保持重要案件的正式资料；

l）水利行政主管部门发布前的水利统计年鉴、资料汇编；

m）全国江河湖泊水文观测数据，统计整编和分析的水文数据等。

18 人口健康

主管部门：卫生计生委。

重要数据包括但不限于：

a）在药品和避孕药具不良反应报告和监测过程中获取的个人隐私、患者和报告者信息；

b）突发公共卫生事件与传染病疫情监测过程中获取的传染病病人及其家属、密切接触者的个人隐私和相关疾病、流行病学信息等；

c）医疗机构和健康管理服务机构保管的个人电子病历、健康档案等各类诊疗、健康数据信息；

d）人体器官移植医疗服务中人体器官捐献者、接受者和人体器官移植手术申请人的个人信息；

e）人类辅助生殖技术服务中精子、卵子捐献者和使用者及人类辅助生殖技

术服务申请人的个人信息；

f）计划生育服务过程中涉及的个人隐私；

g）个人和家族的遗传信息。

19 金融

主管部门：人民银行。

重要数据包括但不限于：

19.1 金融机构安全信息

a）新产品研发方案及研发过程中产生的相关记录和数据；

b）技术方案、电路设计、计算机软件、源代码和目标码、数据库、研究开发记录、技术报告、检测报告、实验数据、实验结果、图纸等技术文档；

c）产品销售信息、市场调研信息、市场营销计划、财务资料、业务分析研究成果等经营资料；

d）客户名单、客户身份资料、客户交易记录等客户资料；

e）内部安全保卫制度、操作细节、银行业务使用的密押、编制方案及专用暗记、代号、指令密码；

f）其他一经泄露会对各金融机构安全和利益造成损害的信息。

19.2 自然人、法人和其他组织金融信息

a）个人财产信息。包括个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金缴存金额等；

b）账户信息。包括银行结算账户和支付账户的信息。主要要素为：账号名称、账号、账户类型、账户开立时间、开户机构、绑定账户信息、账户验证信息（含客户身份外部渠道验证信息）、账户映射的敏感介质信息（如银行卡有效期、验证码、磁道信息等）、账户余额、账户交易情况等；

c）个人信用信息。包括信用卡还款情况、贷款偿还情况及个人在经济活动中形成的，能够反映其信用状况的其他信息；

d）自然人、法人和其他组织金融交易信息。包括银行业金融机构、证券业金融机构、保险业金融机构、交易及结算类金融机构、非银行支付机构等各类金融机构办理业务时获取的自然人、法人和其他组织交易信息；

e）身份信息。包括个人身份信息和单位身份信息。其中个人身份信息包括个人姓名、性别、国籍、民族、身份证种类号码及有效期限、职业、联系方式、婚姻状况、家庭状况、住所或工作单位地址及照片等。单位身份信息包括单位名称、统一社会信用代码、类型、法定代表人（负责人）姓名及身份证件号码、经营场所、联系方式等；

f）衍生信息。包括个人消费习惯、投资意愿等对原始信息进行处理、分析所形成的反映特定个人某些情况的信息；

g）在与自然人、法人和其他组织建立业务关系过程中获取、保存的其他自然人、法人和组织信息。

19.3 中央银行、金融监管部门、外汇管理部门工作中产生的不涉及国家秘密的工作秘密

20 征信

主管部门：人民银行。

重要数据包括以下内容：

a）法院生效判决、裁定、调解和执行信息；

b）欠缴税收信息；

c）欠缴劳动及社会保障保险信息；

d）行政事业性收费、政府性基金欠费信息；

e）公共事业欠费信息；

f）信用卡还款情况、贷款偿还情况；

g）企业和个人与金融机构以外的市场主体发生融资授信关系产生的信息，包括商业信用信息、民间借贷信息和水电费欠费信息等。

21 食品药品

监管部门：食品药品监管总局。

重要数据包括但不限于：

a）涉及国家战略安全的药品在药品审批过程中提交的药品实验数据，例如在动物模型上进行的药理、毒理、稳定性、药代动力学等试验数据，在人体中进行的临床试验数据，以及与药品的生产流程、生产设施有关的试验数据；

b）第二类、第三类医疗器械临床试验数据 / 报告；

c）食品安全溯源标识信息，包括产品名称、执行标准。药品溯源标识信息，包括追溯编码、产品名称、执行标准、配料、生产工艺、标签标识；

d）食品药品安全重大（紧急）信息。包括事件发生时间、地点、当前状况、危害程度、先期处置、发展趋势、事件进展、后续应对措施、调查详情、原因分析；

e）大宗粮食加工品（含大米、小麦粉等）抽检监测信息。

22 统计

主管部门：统计局。

重要数据包括但不限于：

22.1 人口

a）人口普查的资料（包括姓名、性别、年龄、民族、户口登记状况、受教育程度、行业、迁移流动、社会保障、婚姻、生育、死亡、住房情况等）；

b）人口普查中获得的能够识别或者推断单个普查对象身份的资料。

22.2 经济

a）全国国内生产总值（GDP）初步核算数；

b）全国规模以上工业总产值及增加值、主要财务指标；

c）全国单位国内生产总值（GDP）能耗及其降低率；

d）各省、自治区、直辖市单位地区生产总值能耗及其降低率、固定资产投资额、社会消费品零售总额等；

e）各省、自治区、直辖市粮食、棉花总产量；

f）全国粮食、棉花总产量；

g）各省、自治区、直辖市工业生产者出厂价格指数及主要分类指数、购进价格指数及主要分类指数；

h）全国工业生产者出厂价格指数及主要分类指数、购进价格指数及主要分类指数；

i）全国及各省、自治区、直辖市主要工业产品产量；

j）全国及各省、自治区、直辖市房地产开发投资额、销售额、销售面积、建筑业总产值、增加值；

k）全国及各省、自治区、直辖市农林牧渔业总产值、农业生产资料价格指数、商品零售价格指数、固定资产投资价格指数及主要分类指数；

l）全国及各省、自治区、直辖市煤炭等能源消费总量及其增长率；

m）全国及各省、自治区、直辖市农村居民人均现金收入、人均纯收入、人均可支配收入、人均生活消费支出等；

n）全国及各省、自治区、直辖市城镇居民人均可支配收入、人均消费支出；

o）全国及各省、自治区、直辖市居民人均可支配收入、人均消费支出；

p）其他与国家安全和经济利益密切相关的重要统计数据及统计分析材料；

q）其他与全国或较大区域（一省或数省）社会秩序和经济秩序密切相关的重要统计数据及统计分析材料。

23 气象

主管部门：气象局。

重要数据包括但不限于：

a）我国气象卫星原始资料；

b）为国家保密任务或者军事部门保密任务专门设置的气象台站的观测气象数据；

c）为作战、军事演习和训练、国防科研实验等任务专门提供的气象数据；

d）为高科技或者特殊科学试验研究获得的空间大气监测数据；

e）为国家或者军事部门保密任务专门统计整编和分析的重要气象数据；

f）通过非国际交换途径获得的各种国外气象数据；

g）我国未参加国际交换的地面气象、高空气象、气象辐射、大气成分、天气雷达、气象卫星数据及相应元数据，我国未公布的数值预报产品；

h）专项、专业气象数据，包括海洋气象、空间天气、历史气候代用数据、气象灾害数据、航空气象数据、交通气象数据、科学试验考察数据及相应元数据。

24 环境保护

主管部门：环境保护部。

重要数据包括但不限于：

a）未公布的长时间系列各行业（领域）环境污染的重要污染源监测数据和危害程度及重大污染事故情况；

b）未公布的长时间系列大、中城市供水水源的水质资料及主要江湖、河段水质监测资料及监测系统信息；

c）未公布的长时间系列城市空气质量监测资料及相应监测系统信息；

d）未公布的全国土壤污染监测或调查数据。

25 广播电视

主管部门：国家新闻出版广电总局。

重要数据包括但不限于：

a）广播电视安全播出运维、应急保障、调度指挥等信息材料；

b）广播电视监测监管系统产生的相关数据；

c）广播电视台产生业务相关系统网络拓扑、安全运维类信息，以及不宜公开的报道方案、媒体资源类文件等信息资料；

d）广播电视无线和卫星传输覆盖网系统配置、播出参数及台站位置信息等重要数据；

e）全国直播卫星用户信息。

26 海洋环境

主管部门：国家海洋局。

重要数据包括但不限于：

a）海底地形、海洋水文、海洋气象、水声环境和海洋物理场等观测和统计整编数据；

b）领海内的温盐、水声、底质、潮汐、海流实测数据和相关成果；

c）未公布的海洋生态环境监测数据。

27 电子商务

主管部门：商务部。

重要数据包括但不限于：

a）个人在电子商务平台的注册信息，包括姓名、性别、年龄、住址、婚姻、学历、职业、收入、账户、联系方式等；

b）企业在电子商务平台的注册信息，包括企业名称、住址、证照编号、经营范围、账户、联系方式等；

c）电子商务交易记录，以及相关的个人消费习惯及偏好和企业经营数据等；

d）电子商务交易各方的信用记录和信用评价信息；

e）电子商务平台企业的经营数据；

f）电子商务相关服务信息，包括支付和融资信息、物流信息等；

g）对上述数据进行加工形成的涉及国计民生的全国或区域经济运行、行业发展情况的统计分析报告等。

28 其他

重要数据涉及范围众多，本指南仅列出部分行业（领域）重要数据部分范围或内容，其他重要数据可依据下列规则判断、识别：

a）企事业单位掌握的能够反映国家某行业（领域）整体情况的数据，且该行业（领域）与国家安全、社会公共利益密切相关；

b）反映能够导致某行业（领域）发生系统性风险的企事业单位总体运行状况的数据，以及一旦完整性、保密性、可用性遭破坏即能显著影响这些单位稳定运行的各种数据；

c）反映不可更改或长时间保持稳定的自然、经济、社会特征的数据，如地理位置、地貌特征、矿区位置、民族基因特性等；

d）在各类数据集合并过程中能起到识别、关联、连接作用的数据，如地理位置、身份证号、手机号、法人代码；

e）各行业主管部门在重大规划、计划、决策中所依赖或从本行业（领域）的企事业单位调取的部分数据；

f）行政机关、执法机关在履职、执法过程中收集、产生的可能影响国家安全、社会公共利益或存在大量个人隐私的信息；

g）单条或少量信息不会影响国家安全或社会公共利益，但覆盖较大范围或较长时间，一旦出境会带来危害或影响的某些信息集合；

h）单条或少量信息不会影响国家安全或社会公共利益，但涉及某些重要区

域或时期，一旦出境会带来危害或影响的某些信息集合；

i）关键信息基础设施的系统设计、安全防护计划和策略方案，及其单元或设备选型、配置、软件等属性信息和脆弱性信息等；以及包括密码技术在内的其他与国家安全相关的单元、装置、设备、系统或计划、设计能力和缺陷信息；

j）与意识形态、舆情等有关的文化安全相关信息。

行业（领域）主管部门可根据行业（领域）发展、评估实践，判断是否存在其他重要数据并及时更新指南。

附录 D

APPENDIX D

关于发布《网络关键设备和网络安全专用产品目录（第一批）》的公告

为加强网络关键设备和网络安全专用产品安全管理，依据《中华人民共和国网络安全法》，国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会等部门制定了《网络关键设备和网络安全专用产品目录（第一批）》，现予以公布，自印发之日起施行。

一、列入《网络关键设备和网络安全专用产品目录》的设备和产品，应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。

具备资格的机构指国家认证认可监督管理委员会、工业和信息化部、公安部、国家互联网信息办公室按照国家有关规定共同认定的机构。

二、网络关键设备和网络安全专用产品认证或者检测委托人，选择具备资格的机构进行安全认证或者安全检测。

三、网络关键设备、网络安全专用产品选择安全检测方式的，经安全检测符合要求后，由检测机构将网络关键设备、网络安全专用产品检测结果（含本公告发布之前已经本机构安全检测符合要求、且在有效期内的设备与产品）依照相关规定分别报工业和信息化部、公安部。

选择安全认证方式的，经安全认证合格后，由认证机构将认证结果（含本公告发布之前已经本机构安全认证合格、且在有效期内的设备与产品）依照相关规定报国家认证认可监督管理委员会。

国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会统一发布。

特此公告。

附件：网络关键设备和网络安全专用产品目录（第一批）

国家互联网信息办公室 工业和信息化部
公安部 国家认证认可监督管理委员会
2017 年 6 月 1 日

附件：网络关键设备和网络安全专用产品目录（第一批）

	范围	设备或产品类别
网络关键设备	1. 路由器	整系统吞吐量（双向）≥ 12Tbps 整系统路由表容量≥ 55 万条
	2. 交换机	整系统吞吐量（双向）≥ 30Tbps 整系统包转发率≥ 10Gpps
	3. 服务器（机架式）	CPU 数量≥ 8 个 单 CPU 内核数≥ 14 个 内存容量≥ 256GB
	4. 可编程逻辑控制器（PLC 设备）	控制器指令执行时间≤ 0.08μs
网络安全专用产品	5. 数据备份一体机	备份容量≥ 20T 备份速度≥ 60MB/s 备份时间间隔≤ 1h
	6. 防火墙（硬件）	整机吞吐量≥ 80Gbps 最大并发连接数≥ 300 万 每秒新建连接数≥ 25 万
	7. WEB 应用防火墙（WAF）	整机应用吞吐量≥ 6Gbps 最大 HTTP 并发连接数≥ 200 万
	8. 入侵检测系统（IDS）	满检速率≥ 15Gbps 最大并发连接数≥ 500 万
	9. 入侵防御系统（IPS）	满检速率≥ 20Gbps 最大并发连接数≥ 500 万
	10. 安全隔离与信息交换产品（网闸）	吞吐量≥ 1Gbps 系统延时≤ 5ms
	11. 反垃圾邮件产品	连接处理速率（连接 / 秒）>100 平均延迟时间 <100ms
	12. 网络综合审计系统	抓包速度≥ 5Gbps 记录事件能力≥ 5 万条 / 秒
	13. 网络脆弱性扫描产品	最大并行扫描 IP 数量≥ 60 个
	14. 安全数据库系统	TPC-E tpsE（每秒可交易数量）≥ 4500 个
	15. 网站恢复产品（硬件）	恢复时间≤ 2ms 站点的最长路径≥ 10 级

附录 E

APPENDIX E

国家网络安全事件应急预案

中央网信办关于印发《国家网络安全事件应急预案》的通知

中网办发文〔2017〕4号

各省、自治区、直辖市、新疆生产建设兵团党委网络安全和信息化领导小组，中央和国家机关各部委、各人民团体：

《国家网络安全事件应急预案》已经中央网络安全和信息化领导小组同意，现印发给你们，请认真组织实施。

中央网络安全和信息化领导小组办公室

2017年1月10日

1 总则

1.1 编制目的

建立健全国家网络安全事件应急工作机制，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护公众利益，维护国家安全、公共安全和社会秩序。

1.2 编制依据

《中华人民共和国突发事件应对法》、《中华人民共和国网络安全法》、《国家突发公共事件总体应急预案》、《突发事件应急预案管理办法》和《信息安全

技术信息安全事件分类分级指南》（GB/Z 20986-2007）等相关规定。

1.3 适用范围

本预案所指网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，可分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件。

本预案适用于网络安全事件的应对工作。其中，有关信息内容安全事件的应对，另行制定专项预案。

1.4 事件分级

网络安全事件分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。

（1）符合下列情形之一的，为特别重大网络安全事件：

① 重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。

② 国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

③ 其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

（2）符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：

① 重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

② 国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。

③ 其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

（3）符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：

① 重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。

② 国家秘密信息、重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁。

③其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

（4）除上述情形外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

1.5 工作原则

坚持统一领导、分级负责；坚持统一指挥、密切协同、快速反应、科学处置；坚持预防为主，预防与应急相结合；坚持谁主管谁负责、谁运行谁负责，充分发挥各方面力量共同做好网络安全事件的预防和处置工作。

2 组织机构与职责

2.1 领导机构与职责

在中央网络安全和信息化领导小组（以下简称“领导小组”）的领导下，中央网络安全和信息化领导小组办公室（以下简称“中央网信办”）统筹协调组织国家网络安全事件应对工作，建立健全跨部门联动处置机制，工业和信息化部、公安部、国家保密局等相关部门按照职责分工负责相关网络安全事件应对工作。必要时成立国家网络安全事件应急指挥部（以下简称“指挥部”），负责特别重大网络安全事件处置的组织指挥和协调。

2.2 办事机构与职责

国家网络安全应急办公室（以下简称“应急办”）设在中央网信办，具体工

作由中央网信办网络安全协调局承担。应急办负责网络安全应急跨部门、跨地区协调工作和指挥部的事务性工作，组织指导国家网络安全应急技术支撑队伍做好应急处置的技术支撑工作。有关部门派负责相关工作的司局级同志为联络员，联络应急办工作。

2.3 各部门职责

中央和国家机关各部门按照职责和权限，负责本部门、本行业网络和信息系统网络安全事件的预防、监测、报告和应急处置工作。

2.4 各省（区、市）职责

各省（区、市）网信部门在本地区党委网络安全和信息化领导小组统一领导下，统筹协调组织本地区网络和信息系统网络安全事件的预防、监测、报告和应急处置工作。

3 监测与预警

3.1 预警分级

网络安全事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色表示，分别对应发生或可能发生特别重大、重大、较大和一般网络安全事件。

3.2 预警监测

各单位按照“谁主管谁负责、谁运行谁负责”的要求，组织对本单位建设运行的网络和信息系统开展网络安全监测工作。重点行业主管或监管部门组织指导做好本行业网络安全监测工作。各省（区、市）网信部门结合本地区实际，统筹组织开展对本地区网络和信息系统的安全监测工作。各省（区、市）、各部门将重要监测信息报应急办，应急办组织开展跨省（区、市）、跨部门的网络安全信息共享。

3.3 预警研判和发布

各省（区、市）、各部门组织对监测信息进行研判，认为需要立即采取防范

措施的，应当及时通知有关部门和单位，对可能发生重大及以上网络安全事件的信息及时向应急办报告。各省（区、市）、各部门可根据监测研判情况，发布本地区、本行业的橙色及以下预警。

应急办组织研判，确定和发布红色预警和涉及多省（区、市）、多部门、多行业的预警。

预警信息包括事件的类别、预警级别、起始时间、可能影响范围、警示事项、应采取的措施和时限要求、发布机关等。

3.4 预警响应

3.4.1 红色预警响应

（1）应急办组织预警响应工作，联系专家和有关机构，组织对事态发展情况进行跟踪研判，研究制定防范措施和应急工作方案，协调组织资源调度和部门联动的各项准备工作。

（2）有关省（区、市）、部门网络安全事件应急指挥机构实行 24 小时值班，相关人员保持通信联络畅通。加强网络安全事件监测和事态发展信息搜集工作，组织指导应急支撑队伍、相关运行单位开展应急处置或准备、风险评估和控制工作，重要情况报应急办。

（3）国家网络安全应急技术支撑队伍进入待命状态，针对预警信息研究制定应对方案，检查应急车辆、设备、软件工具等，确保处于良好状态。

3.4.2 橙色预警响应

（1）有关省（区、市）、部门网络安全事件应急指挥机构启动相应应急预案，组织开展预警响应工作，做好风险评估、应急准备和风险控制工作。

（2）有关省（区、市）、部门及时将事态发展情况报应急办。应急办密切关注事态发展，有关重大事项及时通报相关省（区、市）和部门。

（3）国家网络安全应急技术支撑队伍保持联络畅通，检查应急车辆、设备、软件工具等，确保处于良好状态。

3.4.3 黄色、蓝色预警响应

有关地区、部门网络安全事件应急指挥机构启动相应应急预案，指导组织开展预警响应。

3.5 预警解除

预警发布部门或地区根据实际情况，确定是否解除预警，及时发布预警解除信息。

4 应急处置

4.1 事件报告

网络安全事件发生后，事发单位应立即启动应急预案，实施处置并及时报送信息。各有关地区、部门立即组织先期处置，控制事态，消除隐患，同时组织研判，注意保存证据，做好信息通报工作。对于初判为特别重大、重大网络安全事件的，立即报告应急办。

4.2 应急响应

网络安全事件应急响应分为四级，分别对应特别重大、重大、较大和一般网络安全事件。I级为最高响应级别。

4.2.1 Ⅰ级响应

属特别重大网络安全事件的，及时启动I级响应，成立指挥部，履行应急处置工作的统一领导、指挥、协调职责。应急办24小时值班。

有关省（区、市）、部门应急指挥机构进入应急状态，在指挥部的统一领导、指挥、协调下，负责本省（区、市）、本部门应急处置工作或支援保障工作，24小时值班，并派员参加应急办工作。

有关省（区、市）、部门跟踪事态发展，检查影响范围，及时将事态发展变化情况、处置进展情况报应急办。指挥部对应对工作进行决策部署，有关省（区、市）和部门负责组织实施。

4.2.2 Ⅱ级响应

网络安全事件的Ⅱ级响应，由有关省（区、市）和部门根据事件的性质和情况确定。

（1）事件发生省（区、市）或部门的应急指挥机构进入应急状态，按照相关应急预案做好应急处置工作。

（2）事件发生省（区、市）或部门及时将事态发展变化情况报应急办。应急办将有关重大事项及时通报相关地区和部门。

（3）处置中需要其他有关省（区、市）、部门和国家网络安全应急技术支撑队伍配合和支持的，商应急办予以协调。相关省（区、市）、部门和国家网络安全应急技术支撑队伍应根据各自职责，积极配合、提供支持。

（4）有关省（区、市）和部门根据应急办的通报，结合各自实际有针对性地加强防范，防止造成更大范围影响和损失。

4.2.3 Ⅲ级、Ⅳ级响应

事件发生地区和部门按相关预案进行应急响应。

4.3 应急结束

4.3.1 Ⅰ级响应结束

应急办提出建议，报指挥部批准后，及时通报有关省（区、市）和部门。

4.3.2 Ⅱ级响应结束

由事件发生省（区、市）或部门决定，报应急办，应急办通报相关省（区、市）和部门。

5 调查与评估

特别重大网络安全事件由应急办组织有关部门和省（区、市）进行调查处理和总结评估，并按程序上报。重大及以下网络安全事件由事件发生地区或部门自行组织调查处理和总结评估，其中重大网络安全事件相关总结调查报告报应急办。总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。

事件的调查处理和总结评估工作原则上在应急响应结束后 30 天内完成。

6 预防工作

6.1 日常管理

各地区、各部门按职责做好网络安全事件日常预防工作，制定完善相关应急预案，做好网络安全检查、隐患排查、风险评估和容灾备份，健全网络安全信息通报机制，及时采取有效措施，减少和避免网络安全事件的发生及危害，提高应对网络安全事件的能力。

6.2 演练

中央网信办协调有关部门定期组织演练，检验和完善预案，提高实战能力。

各省（区、市）、各部门每年至少组织一次预案演练，并将演练情况报中央网信办。

6.3 宣传

各地区、各部门应充分利用各种传播媒介及其他有效的宣传形式，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传，开展网络安全基本知识和技能的宣传活动。

6.4 培训

各地区、各部门要将网络安全事件的应急知识列为领导干部和有关人员的培训内容，加强网络安全特别是网络安全应急预案的培训，提高防范意识及技能。

6.5 重要活动期间的预防措施

在国家重要活动、会议期间，各省（区、市）、各部门要加强网络安全事件的防范和应急响应，确保网络安全。应急办统筹协调网络安全保障工作，根据需要要求有关省（区、市）、部门启动红色预警响应。有关省（区、市）、部门加强网络安全监测和分析研判，及时预警可能造成重大影响的风险和隐患，重点部门、重点岗位保持24小时值班，及时发现和处置网络安全事件隐患。

7 保障措施

7.1 机构和人员

各地区、各部门、各单位要落实网络安全应急工作责任制，把责任落实到具体部门、具体岗位和个人，并建立健全应急工作机制。

7.2 技术支撑队伍

加强网络安全应急技术支撑队伍建设，做好网络安全事件的监测预警、预防防护、应急处置、应急技术支援工作。支持网络安全企业提升应急处置能力，提供应急技术支援。中央网信办制定评估认定标准，组织评估和认定国家网络安全应急技术支撑队伍。各省（区、市）、各部门应配备必要的网络安全专业技术人才，并加强与国家网络安全相关技术单位的沟通、协调，建立必要的网络安全信息共享机制。

7.3 专家队伍

建立国家网络安全应急专家组，为网络安全事件的预防和处置提供技术咨询和决策建议。各地区、各部门加强各自的专家队伍建设，充分发挥专家在应急处置工作中的作用。

7.4 社会资源

从教育科研机构、企事业单位、协会中选拔网络安全人才，汇集技术与数据资源，建立网络安全事件应急服务体系，提高应对特别重大、重大网络安全事件的能力。

7.5 基础平台

各地区、各部门加强网络安全应急基础平台和管理平台建设，做到早发现、早预警、早响应，提高应急处置能力。

7.6 技术研发和产业促进

有关部门加强网络安全防范技术研究，不断改进技术装备，为应急响应工作提供技术支撑。加强政策引导，重点支持网络安全监测预警、预防防护、处置救援、应急服务等方向，提升网络安全应急产业整体水平与核心竞争力，增强防范和处置网络安全事件的产业支撑能力。

7.7 国际合作

有关部门建立国际合作渠道，签订合作协定，必要时通过国际合作共同应对突发网络安全事件。

7.8 物资保障

加强对网络安全应急装备、工具的储备，及时调整、升级软件硬件工具，不断增强应急技术支撑能力。

7.9 经费保障

财政部门为网络安全事件应急处置提供必要的资金保障。有关部门利用现有政策和资金渠道，支持网络安全应急技术支撑队伍建设、专家队伍建设、基础平台建设、技术研发、预案演练、物资保障等工作开展。各地区、各部门为网络安全应急工作提供必要的经费保障。

7.10 责任与奖惩

网络安全事件应急处置工作实行责任追究制。

中央网信办及有关地区和部门对网络安全事件应急管理工作中作出突出贡献的先进集体和个人给予表彰和奖励。

中央网信办及有关地区和部门对不按照规定制定预案和组织开展演练，迟报、谎报、瞒报和漏报网络安全事件重要情况或者应急管理工作中有其他失职、渎职行为的，依照相关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

8 附则

8.1 预案管理

本预案原则上每年评估一次，根据实际情况适时修订。修订工作由中央网信办负责。

各省（区、市）、各部门、各单位要根据本预案制定或修订本地区、本部门、本行业、本单位网络安全事件应急预案。

8.2 预案解释

本预案由中央网信办负责解释。

8.3 预案实施时间

本预案自印发之日起实施。

附件：

1. 网络安全事件分类
2. 名词术语
3. 网络和信息系统损失程度划分说明

附件1 网络安全事件分类

网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等。

（1）有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件。

（2）网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

（3）信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

（4）信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

（5）设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

（6）灾害性事件是指由自然灾害等其他突发事件导致的网络安全事件。

（7）其他事件是指不能归为以上分类的网络安全事件。

附件 2　名词术语

一、重要网络与信息系统

所承载的业务与国家安全、社会秩序、经济建设、公众利益密切相关的网络和信息系统。

（参考依据：《信息安全技术信息安全事件分类分级指南》（GB/Z 20986-2007））

二、重要敏感信息

不涉及国家秘密，但与国家安全、经济发展、社会稳定以及企业和公众利益密切相关的信息，这些信息一旦未经授权披露、丢失、滥用、篡改或销毁，可能造成以下后果：

a）损害国防、国际关系；

b）损害国家财产、公共利益以及个人财产或人身安全；

c）影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；

d）影响行政机关依法调查处理违法、渎职行为，或涉嫌违法、渎职行为；

e）干扰政府部门依法公正地开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；

f）危害国家关键基础设施、政府信息系统安全；

g）影响市场秩序，造成不公平竞争，破坏市场规律；

h）可推论出国家秘密事项；

i）侵犯个人隐私、企业商业秘密和知识产权；

j）损害国家、企业、个人的其他利益和声誉。

（参考依据：《信息安全技术云计算服务安全指南》（GB/T31167-2014））

附件 3　网络和信息系统损失程度划分说明

网络和信息系统损失是指由于网络安全事件对系统的软硬件、功能及数据的破坏，导致系统业务中断，从而给事发组织所造成的损失，其大小主要考虑恢复系统正常运行和消除安全事件负面影响所需付出的代价，划分为特别严重的系统损失、严重的系统损失、较大的系统损失和较小的系统损失，说明如下：

a）特别严重的系统损失：造成系统大面积瘫痪，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价十分巨大，对于事发组织是不可承受的；

b）严重的系统损失：造成系统长时间中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价巨大，但对于事发组织是可承受的；

c）较大的系统损失：造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到破坏，恢复系统正常运行和消除安全事件负面影响所需付出的代价较大，但对于事发组织是完全可以承受的；

d）较小的系统损失：造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响，恢复系统正常运行和消除安全事件负面影响所需付出的代价较小。

附录 F

APPENDIX F

关键信息基础设施安全保护条例（征求意见稿）

第一章　总则

第一条　为了保障关键信息基础设施安全，根据《中华人民共和国网络安全法》，制定本条例。

第二条　在中华人民共和国境内规划、建设、运营、维护、使用关键信息基础设施，以及开展关键信息基础设施的安全保护，适用本条例。

第三条　关键信息基础设施安全保护坚持顶层设计、整体防护，统筹协调、分工负责的原则，充分发挥运营主体作用，社会各方积极参与，共同保护关键信息基础设施安全。

第四条　国家行业主管或监管部门按照国务院规定的职责分工，负责指导和监督本行业、本领域的关键信息基础设施安全保护工作。

国家网信部门负责统筹协调关键信息基础设施安全保护工作和相关监督管理工作。国务院公安、国家安全、国家保密行政管理、国家密码管理等部门在各自职责范围内负责相关网络安全保护和监督管理工作。

县级以上地方人民政府有关部门按照国家有关规定开展关键信息基础设施安全保护工作。

第五条　关键信息基础设施的运营者（以下称运营者）对本单位关键信息基础设施安全负主体责任，履行网络安全保护义务，接受政府和社会监督，承担社会责任。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第六条　关键信息基础设施在网络安全等级保护制度基础上，实行重点保护。

第七条　任何个人和组织发现危害关键信息基础设施安全的行为，有权向网信、电信、公安等部门以及行业主管或监管部门举报。

收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章　支持与保障

第八条　国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动。

第九条　国家制定产业、财税、金融、人才等政策，支持关键信息基础设施安全相关的技术、产品、服务创新，推广安全可信的网络产品和服务，培养和选拔网络安全人才，提高关键信息基础设施的安全水平。

第十条　国家建立和完善网络安全标准体系，利用标准指导、规范关键信息基础设施安全保护工作。

第十一条　地市级以上人民政府应当将关键信息基础设施安全保护工作纳入地区经济社会发展总体规划，加大投入，开展工作绩效考核评价。

第十二条　国家鼓励政府部门、运营者、科研机构、网络安全服务机构、行业组织、网络产品和服务提供者开展关键信息基础设施安全合作。

第十三条　国家行业主管或监管部门应当设立或明确专门负责本行业、本领域关键信息基础设施安全保护工作的机构和人员，编制并组织实施本行业、本领域的网络安全规划，建立健全工作经费保障机制并督促落实。

第十四条　能源、电信、交通等行业应当为关键信息基础设施网络安全事件应急处置与网络功能恢复提供电力供应、网络通信、交通运输等方面的重点保障和支持。

第十五条　公安机关等部门依法侦查打击针对和利用关键信息基础设施实施的违法犯罪活动。

第十六条　任何个人和组织不得从事下列危害关键信息基础设施的活动和行为：

（一）攻击、侵入、干扰、破坏关键信息基础设施；

（二）非法获取、出售或者未经授权向他人提供可能被专门用于危害关键信息基础设施安全的技术资料等信息；

（三）未经授权对关键信息基础设施开展渗透性、攻击性扫描探测；

（四）明知他人从事危害关键信息基础设施安全的活动，仍然为其提供互联网接入、服务器托管、网络存储、通讯传输、广告推广、支付结算等帮助；

（五）其他危害关键信息基础设施的活动和行为。

第十七条 国家立足开放环境维护网络安全，积极开展关键信息基础设施安全领域的国际交流与合作。

第三章 关键信息基础设施范围

第十八条 下列单位运行、管理的网络设施和信息系统，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的，应当纳入关键信息基础设施保护范围：

（一）政府机关和能源、金融、交通、水利、卫生医疗、教育、社保、环境保护、公用事业等行业领域的单位；

（二）电信网、广播电视网、互联网等信息网络，以及提供云计算、大数据和其他大型公共信息网络服务的单位；

（三）国防科工、大型装备、化工、食品药品等行业领域科研生产单位；

（四）广播电台、电视台、通讯社等新闻单位；

（五）其他重点单位。

第十九条 国家网信部门会同国务院电信主管部门、公安部门等部门制定关键信息基础设施识别指南。

国家行业主管或监管部门按照关键信息基础设施识别指南，组织识别本行业、本领域的关键信息基础设施，并按程序报送识别结果。

关键信息基础设施识别认定过程中，应当充分发挥有关专家作用，提高关键信息基础设施识别认定的准确性、合理性和科学性。

第二十条 新建、停运关键信息基础设施，或关键信息基础设施发生重大变化的，运营者应当及时将相关情况报告国家行业主管或监管部门。

国家行业主管或监管部门应当根据运营者报告的情况及时进行识别调整，并按程序报送调整情况。

第四章　运营者安全保护

第二十一条　建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第二十二条　运营者主要负责人是本单位关键信息基础设施安全保护工作第一责任人，负责建立健全网络安全责任制并组织落实，对本单位关键信息基础设施安全保护工作全面负责。

第二十三条　运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障关键信息基础设施免受干扰、破坏或者未经授权的访问，防止网络数据泄漏或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，严格身份认证和权限管理；

（二）采取技术措施，防范计算机病毒和网络攻击、网络侵入等危害网络安全行为；

（三）采取技术措施，监测、记录网络运行状态、网络安全事件，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密认证等措施。

第二十四条　除本条例第二十三条外，运营者还应当按照国家法律法规的规定和相关国家标准的强制性要求，履行下列安全保护义务：

（一）设置专门网络安全管理机构和网络安全管理负责人，并对该负责人和关键岗位人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份，及时对系统漏洞等安全风险采取补救措施；

（四）制定网络安全事件应急预案并定期进行演练；

（五）法律、行政法规规定的其他义务。

第二十五条　运营者网络安全管理负责人履行下列职责：

（一）组织制定网络安全规章制度、操作规程并监督执行；

（二）组织对关键岗位人员的技能考核；

（三）组织制定并实施本单位网络安全教育和培训计划；

（四）组织开展网络安全检查和应急演练，应对处置网络安全事件；

（五）按规定向国家有关部门报告网络安全重要事项、事件。

第二十六条 运营者网络安全关键岗位专业技术人员实行执证上岗制度。

执证上岗具体规定由国务院人力资源社会保障部门会同国家网信部门等部门制定。

第二十七条 运营者应当组织从业人员网络安全教育培训，每人每年教育培训时长不得少于 1 个工作日，关键岗位专业技术人员每人每年教育培训时长不得少于 3 个工作日。

第二十八条 运营者应当建立健全关键信息基础设施安全检测评估制度，关键信息基础设施上线运行前或者发生重大变化时应当进行安全检测评估。

运营者应当自行或委托网络安全服务机构对关键信息基础设施的安全性和可能存在的风险隐患每年至少进行一次检测评估，对发现的问题及时进行整改，并将有关情况报国家行业主管或监管部门。

第二十九条 运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照个人信息和重要数据出境安全评估办法进行评估；法律、行政法规另有规定的，依照其规定。

第五章 产品和服务安全

第三十条 运营者采购、使用的网络关键设备、网络安全专用产品，应当符合法律、行政法规的规定和相关国家标准的强制性要求。

第三十一条 运营者采购网络产品和服务，可能影响国家安全的，应当按照网络产品和服务安全审查办法的要求，通过网络安全审查，并与提供者签订安全保密协议。

第三十二条 运营者应当对外包开发的系统、软件，接受捐赠的网络产品，在其上线应用前进行安全检测。

第三十三条 运营者发现使用的网络产品、服务存在安全缺陷、漏洞等风险的，应当及时采取措施消除风险隐患，涉及重大风险的应当按规定向有关部门报告。

第三十四条 关键信息基础设施的运行维护应当在境内实施。因业务需要，确需进行境外远程维护的，应事先报国家行业主管或监管部门和国务院公安部门。

第三十五条 面向关键信息基础设施开展安全检测评估，发布系统漏洞、计算机病毒、网络攻击等安全威胁信息，提供云计算、信息技术外包等服务的机构，应当符合有关要求。

具体要求由国家网信部门会同国务院有关部门制定。

第六章 监测预警、应急处置和检测评估

第三十六条 国家网信部门统筹建立关键信息基础设施网络安全监测预警体系和信息通报制度，组织指导有关机构开展网络安全信息汇总、分析研判和通报工作，按照规定统一发布网络安全监测预警信息。

第三十七条 国家行业主管或监管部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警和信息通报制度，及时掌握本行业、本领域关键信息基础设施运行状况和安全风险，向有关运营者通报安全风险和相关工作信息。

国家行业主管或监管部门应当组织对安全监测信息进行研判，认为需要立即采取防范应对措施的，应当及时向有关运营者发布预警信息和应急防范措施建议，并按照国家网络安全事件应急预案的要求向有关部门报告。

第三十八条 国家网信部门统筹协调有关部门、运营者以及有关研究机构、网络安全服务机构建立关键信息基础设施网络安全信息共享机制，促进网络安全信息共享。

第三十九条 国家网信部门按照国家网络安全事件应急预案的要求，统筹有关部门建立健全关键信息基础设施网络安全应急协作机制，加强网络安全应急力量建设，指导协调有关部门组织跨行业、跨地域网络安全应急演练。

国家行业主管或监管部门应当组织制定本行业、本领域的网络安全事件应急预案，并定期组织演练，提升网络安全事件应对和灾难恢复能力。发生重大网络安全事件或接到网信部门的预警信息后，应立即启动应急预案组织应对，并及时报告有关情况。

第四十条 国家行业主管或监管部门应当定期组织对本行业、本领域关键信息基础设施的安全风险以及运营者履行安全保护义务的情况进行抽查检测，提出改进措施，指导、督促运营者及时整改检测评估中发现的问题。

国家网信部门统筹协调有关部门开展的抽查检测工作，避免交叉重复检测评估。

第四十一条 有关部门组织开展关键信息基础设施安全检测评估，应坚持客观公正、高效透明的原则，采取科学的检测评估方法，规范检测评估流程，控制检测评估风险。

运营者应当对有关部门依法实施的检测评估予以配合，对检测评估发现的问题及时进行整改。

第四十二条 有关部门组织开展关键信息基础设施安全检测评估，可采取下列措施：

（一）要求运营者相关人员就检测评估事项作出说明；

（二）查阅、调取、复制与安全保护有关的文档、记录；

（三）查看网络安全管理制度制订、落实情况以及网络安全技术措施规划、建设、运行情况；

（四）利用检测工具或委托网络安全服务机构进行技术检测；

（五）经运营者同意的其他必要方式。

第四十三条 有关部门以及网络安全服务机构在关键信息基础设施安全检测评估中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第四十四条 有关部门组织开展关键信息基础设施安全检测评估，不得向被检测评估单位收取费用，不得要求被检测评估单位购买指定品牌或者指定生产、销售单位的产品和服务。

第七章　法律责任

第四十五条　运营者不履行本条例第二十条第一款、第二十一条、第二十三条、第二十四条、第二十六条、第二十七条、第二十八条、第三十条、第三十二条、第三十三条、第三十四条规定的网络安全保护义务的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

第四十六条　运营者违反本条例第二十九条规定，在境外存储网络数据，或者向境外提供网络数据的，由国家有关主管部门依据职责责令改正，给予警告，没收违法所得，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第四十七条　运营者违反本条例第三十一条规定，使用未经安全审查或安全审查未通过的网络产品或者服务的，由国家有关主管部门依据职责责令停止使用，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第四十八条　个人违反本条例第十六条规定，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款；构成犯罪的，依法追究刑事责任。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本条例第十六条规定，受到刑事处罚的人员，终身不得从事关键信息基础设施安全管理和网络运营关键岗位的工作。

第四十九条　国家机关关键信息基础设施的运营者不履行本条例规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接负责人员依法给予处分。

第五十条　有关部门及其工作人员有下列行为之一的，对直接负责的主管人

员和其他直接责任人员依法给予处分；构成犯罪的，依法追究刑事责任：

（一）在工作中利用职权索取、收受贿赂；

（二）玩忽职守、滥用职权；

（三）擅自泄露关键信息基础设施有关信息、资料及数据文件；

（四）其他违反法定职责的行为。

第五十一条 关键信息基础设施发生重大网络安全事件，经调查确定为责任事故的，除应当查明运营单位责任并依法予以追究外，还应查明相关网络安全服务机构及有关部门的责任，对有失职、渎职及其他违法行为的，依法追究责任。

第五十二条 境外的机构、组织、个人从事攻击、侵入、干扰、破坏等危害中华人民共和国的关键信息基础设施的活动，造成严重后果的，依法追究法律责任；国务院公安部门、国家安全机关和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第八章 附则

第五十三条 存储、处理涉及国家秘密信息的关键信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。

关键信息基础设施中的密码使用和管理，还应当遵守密码法律、行政法规的规定。

第五十四条 军事关键信息基础设施的安全保护，由中央军事委员会另行规定。

第五十五条 本条例自 **** 年 ** 月 ** 日起施行。